LAS MEDIDAS DE INVESTIGACIÓN TECNOLÓGICA EN EL PROCESO PENAL ESPAÑOL

TECHNOLOGICAL RESEARCH MEASURES IN THE SPANISH CRIMINAL PROCESS

Máster Universitario en Acceso a la Profesión de Abogado

Presentado por:

Dª SANDRA PRIETO AGUADO

Dirigido por Dr. D. ESTEBAN MESTRE DELGADO

Co-Dirigido por Dr. D. MIGUEL MARCOS AYJÓN

Alcalá de Henares, a 3 de marzo de 2020

RESUMEN

La utilización de los avances tecnológicos que han ido surgiendo en los últimos años, en las tareas de investigación del delito por parte de las Fuerzas y Cuerpos de Seguridad del Estado, resulta esencial para la persecución y resolución de los ilícitos, especialmente en aquellos en los que la tecnología juega un papel fundamental, y, por lo tanto, dicho empleo representa el presente y el futuro de la actividad policial. Consecuentemente, la legislación procesal española, a partir de la jurisprudencia, ha desarrollado las necesidades urgentes sobre cómo, dónde y cuándo aplicar las nuevas medidas tecnológicas de investigación criminal con las debidas garantías. En el presente trabajo se analiza la nueva legislación referente a las medidas de investigación que suponen una injerencia en los derechos contenidos en el artículo 18 de la Constitución Española, así como a las disposiciones específicas sobre el uso de dispositivos técnicos de captación de imágenes y de dispositivos técnicos de seguimiento y localización, como medidas para la investigación penal. A su vez, se expondrán los Derechos Fundamentales afectados.

ABSTRACT

The use of technological advances that have emerged in recent years, in the tasks of investigating crime by the State's security forces, is essential for the prosecution and resolution of illicit acts, especially in those in which technology plays a major role, and therefore, such use represents the present and future of police activity. Consequently, Spanish procedural legislation, through case law, has developed and met the urgent needs on how, where and when to apply new technological measures of criminal investigation with due guarantees. This paper analyses the new legislation concerning the provisions common to the restrictive measures of Article 18 of the Spanish Constitution, as well as the specific provisions on the use of technical devices for capturing images and technical devices for tracking and tracing, as measures for criminal investigation. In turn, the Fundamental Rights affected will be set out.

PALABRAS CLAVE

Autorización judicial.
Cámaras de videovigilancia.
Dispositivos técnicos de captación de imagen.
Dispositivos técnicos de seguimiento y geolocalización.
Derecho al entorno virtual.
Derechos fundamentales.
Derecho a la intimidad.
Derecho a la protección de datos.
Derecho al secreto de las comunicaciones.
Lugares o espacios públicos.
Policía Judicial.
Prueba preconstituida.

KEY WORDS

Fundamental rights.
Judicial authorization.
Judicial Police.
Pre-constituted evidence.
Public places or spaces.
Right to data protection.
Right to privacy.
Right to the secrecy of communications.
Right to the virtual environment.
Technical devices for image capture.
Technical devices for tracking and geolocation.
Video surveillance cameras.

ABREVIATURAS

AEPD: Agencia Española de Protección de datos.

Art.: Artículo

BOE: Boletín Oficial del Estado.

CE: Constitución Española

CEDH: Convenio Europeo de Derechos Humanos

FGE: Fiscalía General del Estado.

FJ: Fundamento Jurídico de una Sentencia

GSM: Sistema global de comunicaciones

LECRIM: Real Decreto de 14 de septiembre de 1882, por el que se aprueba la Ley de Enjuiciamiento Criminal

LOMLECRIM: Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica

LO: Ley Orgánica.

LOPD: Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal

LOPJ: Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial

LOPDPGDD: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

LOPSC: Ley Orgánica 4/2015, de 30 de marzo, de Protección de la Seguridad Ciudadana

LORTAD: Ley 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal

Núm.: número.

pp.: páginas

RD: Real Decreto

SITEL: Sistema de escuchas telefónicas del Ministerio del Interior

STC: Sentencia del Tribunal Constitucional

STEDH: Sentencia del Tribunal Europeo de Derechos Humanos

STJUE: Sentencia del Tribunal de Justicia de la Unión Europea

STS: Sentencia del Tribunal Supremo.

TEDH: Tribunal Europeo de Derechos Humanos

INTRODUCCIÓN

La LOMLECRIM, ha surgido de la necesidad de implantar nuevos métodos o herramientas de investigación, ya que la forma de aplicar determinados métodos o instrumentos tecnológicos se estaba dejando al arbitrio judicial, que venía reclamando una normativa para ello; por ello, el Tribunal Constitucional subrayó la exigencia perentoria de una nueva legislación que afrontase la injerencia en la privacidad de la persona investigada con las debidas garantías constitucionales, para evitar la incidencia negativa que ciertas realidades están proyectando sobre algunos de los derechos fundamentales.

A su vez, la exigencia de autorización judicial para realizar actos de investigación que pudiesen limitar derechos fundamentales reconocidos en el art. 18 CE satisface las necesidades surgidas en la fase de instrucción para afrontar las nuevas formas de delincuencia nacidas de la progresión tecnológica. Por ello, resulta adecuado, concretar el contenido de la CE y de las garantías en cuanto al procedimiento para que no se vulneren los derechos fundamentales, y hacer patente la falta de previsión constitucional para delimitar de forma restrictiva el tratamiento de todos ellos[1].

Hasta la promulgación de la LOMLECRIM, no existían unos antecedentes legales específicos sobre los medios tecnológicos que puede utilizar la Policía Judicial para investigar los delitos, y que pueden conllevar la injerencia o limitación de los derechos fundamentales instaurados en el art. 18 de la CE. Las diversas Instrucciones de la Fiscalía General del Estado vienen a arrojar luz sobre la aplicación de las medidas introducidas en la citada reforma.

En este trabajo se analizarán las medidas de investigación implementadas en la reforma efectuada por la LOMLECRIM, pero concretando el estudio en las medidas referentes al uso de dispositivos técnicos de captación de imágenes y de seguimiento y localización, ya que me parecen más novedosas que el resto y por el juego que supone el cambio de una sola circunstancia para que estas medidas invadan Derechos Fundamentales, con la consiguiente nulidad de la prueba obtenida de considerarse ilícita.

[1] ZOCO ZABALA, C.: *Nuevas tecnologías y control de las comunicaciones.* Editorial Aranzadi, S.A., Pamplona (Navarra), Primera edición, 2015, Pp. 38-39.

En la investigación de los delitos, la Policía Judicial deberá no transgredir los derechos inherentes a cada persona y que están reconocidos por la Constitución, siendo la encargada de la práctica de las diligencias necesarias para recoger los vestigios del delito y las pruebas necesarias que permitan descubrir a los delincuentes. Ahora bien, cuando realiza esta función no puede violentar los derechos o libertades fundamentales, porque, de hacerlo, se procederá al rechazo de la prueba por los órganos judiciales que declararán su nulidad de acuerdo con el art. 11 de la Ley Orgánica del Poder Judicial[2].

Para el presente trabajo se utilizará un método técnico-jurídico en el que se abordarán de forma concreta las dos medidas anteriores, desde la instancia normativa y jurisprudencial, para tratar de verificar cuáles son los problemas que se producen, a fin de proponer soluciones.

[2] STS 610/2016, de 7 de julio, FJ 1º

CAPÍTULO I: LOS DERECHOS FUNDAMENTALES PROTEGIDOS EN EL ART. 18 DE LA CE Y EL PROCESO PENAL

En la actualidad, la investigación policial e instrucción judicial se sirven de los medios tecnológicos para constatar los vestigios de la comisión de los delitos, ya que aquéllos permiten nuevas formas de investigación. La LOMLECRIM permite la utilización de estos medios, en nuestro enfoque, el uso de dispositivos técnicos de captación de imágenes y de dispositivos técnicos de seguimiento y localización, que en ocasiones conllevan la injerencia en los derechos contenidos en el art. 18 CE; concretamente el derecho fundamental a la intimidad (18.1 CE), el secreto de las comunicaciones (18.3 CE) y en la protección de datos de carácter personal (18.4 CE).

A continuación, vamos a conocer lo que la jurisprudencia establece sobre el significado de estos derechos.

1.1 Derecho a la intimidad (18.1 CE)

El derecho a la intimidad garantiza al individuo un dominio legal sobre la información relativa a su persona o a su familia, que permite imponer a terceros, particulares o poderes públicos, su deseo de excluirlos del conocimiento de su información o vedando la difusión de la misma por no mediar su consentimiento.

En el caso de las certificaciones de antecedentes penales, el Tribunal Constitucional señala que únicamente podrán ser requeridas *"por el interesado o por los órganos judiciales u otros poderes públicos cuando así lo disponga una norma con rango legal. Fuera de estos casos, y dada la naturaleza de los datos contenidos en el referido Registro*[3]*, el acceso a ellos vulnera el derecho a la intimidad"* de la persona a quien el documento atribuya los antecedentes, y afectan a su integridad moral. La justificación del acceso sólo está justificada si el motivo coincide con alguna de las limitaciones que la CE asigna a la esfera íntima del individuo y su familia[4]. Asimismo, el tratamiento de los datos de naturaleza penal, siguiendo el art. 10 LOPDGDD, solo será posible por los

[3] Registro Central de Penados y Rebeldes.
[4] Sala Segunda. STC 144/1999, de 22 de julio (BOE núm. 204 de 22 de agosto de 1999), FJ 8º.

abogados y procuradores cuando la finalidad que persiguen estos sea recoger la información proporcionada por sus clientes para poder ejercer sus funciones.

No se le puede pedir a ninguna persona que soporte sin oposición la revelación de datos, reales o supuestos, de su vida privada, personal o familiar[5]. Habrán de analizarse en cada caso concreto los sucesos y el vínculo que atañe a las personas objeto de discusión, pero no puede dudarse de que ciertos hechos que le sucedan a familiares, como padres, cónyuges o hijos de una persona, tienen tal importancia para el sujeto, dentro de nuestras pautas culturales, que si son indebidamente publicitados o difundidos, a través de la televisión o de grabaciones, afectarán de forma directa en la propia esfera la personalidad, existiendo un derecho propio y no ajeno a la intimidad, susceptible de tutela constitucional.

La Constitución recoge el derecho a la intimidad en el art. 18.1[6], y tiene su desarrollo legislativo en la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, sin perjuicio de la protección penal que, en su caso, pueda también ampararlos.

El requisito ineludible para obtener la tutela prevista en esta Ley es que el presunto acto lesivo del derecho no cuente con la autorización del sujeto, según el art. 2.2 de la LO mencionada supra, consentimiento revocable en cualquier momento, en virtud del art. 2.3. Cuando se vulnera cualquiera de los derechos, sea al honor, a la intimidad o a la propia imagen, y se pueda acreditar una intromisión ilegítima conforme a las distintas situaciones previstas en el art. 7, será posible obtener una indemnización. Para evaluar esta, el órgano judicial analizará el daño moral, la gravedad de la lesión y el beneficio alcanzado por el causante.

Es imprescindible mencionar el **Caso López Ribalda y otros contra España**, en el cual varias trabajadoras de una cadena de supermercados interpusieron varias demandas alegando que habían sido vigiladas por cámaras sin que su empleador[7] se lo

[5] Sala Segunda. STC 115/2000, de 5 de mayo (BOE núm. 136 de 07 de junio de 2000), FJ 4º.
[6] Sala Segunda. STC 231/1988, de 2 de diciembre (BOE núm. 307 de 23 de diciembre de 1988), FJ 4º.
[7] Instaló tanto cámaras visibles como ocultas, que apuntaban a los mostradores de salida y cubrían la zona de detrás de las cajas registradoras, con el objetivo de investigar y acabar con las pérdidas económicas, por el desajuste que se produjo en varios meses entre el stock existente y lo que realmente se vendía.

hubiera comunicado de forma previa, y que esto suponía una violación de su derecho a la privacidad del art. 8 del CEDH. También consideraban esto respecto del art. 6 CEDH, ya que, según ellas, los procedimientos judiciales llevados a cabo en los Tribunales nacionales fueron injustos, pues la grabación fue usada como prueba única y principal para justificar la procedencia de los despidos.

El TEDH se plantea, **en su primera Sentencia**[8], primordialmente y respecto al derecho que nos ocupa, si el Estado, en ejercicio del art. 8 CEDH, logró efectuar una ponderación ecuánime entre el derecho de las demandantes al respeto que merecen sus vidas privadas y el interés del empleador en preservar sus derechos en cuanto a organización y gestión en lo respecta al derecho a la propiedad, así como al interés público sobre la correcta administración de la justicia[9].

El empleador no informó previamente, de modo expreso, preciso e inequívoco acerca de la videovigilancia, como requiere el art. 89.1 de la LOPDPGDD, que no solo estaba dirigida a las demandantes, sino a todo el personal, grabando durante todo el horario laboral. La sospecha era generalizada, y fue comunicada por el encargado al empleador. El medio menos lesivo que podía haber utilizado era haber informado de forma general de un sistema de videovigilancia y hacerles referencia a la LOPD, para así haber podido salvaguardar sus derechos; por todo ello, el Tribunal considera vulnerado el art. 8 CEDH, a diferencia de los Tribunales nacionales.

Respecto a que la grabación fue utilizada como prueba única y principal para fundamentar los despidos, el Tribunal ha podido observar que no solo se tomó aquélla en cuenta, sino, también, las declaraciones como testigos de las compañeras de trabajo también despedidas por su participación en los robos, el coordinador de tienda, el delegado sindical y el representante legal de la empresa, por lo que las pruebas en conjunto son perfectamente válidas, y avalan la procedencia del despido. A su vez, señala que existe vulneración de la privacidad de las demandantes y condena al Estado español a indemnizar a las cajeras despedidas por no haber sido previamente avisadas de la grabación de las cámaras ocultas.

[8] Sentencia del Tribunal Europeo de Derechos Humanos, de 9 de enero de 2018, asunto López Ribalda y otros contra España. Disponible en: https://www.icav.es/bd/archivos/archivo11428.pdf . Consultada el 5 de febrero de 2020.
[9] TEDH II. Argumentos 60-70.

De otro lado, tenemos la **segunda Sentencia**[10] del Caso, pues el Gobierno solicitó al TEDH que examinara de nuevo la vulneración del art. 8 del CEDH, aceptando esta petición la Gran Sala del TEDH, pues, como objeción preliminar, se dice que el Gobierno mantuvo que las demandantes no habían agotado los recursos disponibles en el derecho interno, como son una queja ante el Organismo de Protección de Datos, en el caso de España la AEPD, o la iniciación de un procedimiento penal, que podían haber acarreado sanción administrativa o penal al empleador.

La protección de la "vida privada" no puede extenderse a la conducta delictiva. Ese concepto abarca el derecho a llevar una "vida social privada", es decir, la posibilidad de crear y desenvolver relaciones con otras personas y con el mundo exterior, existiendo, pues, un área donde pueda interactuar con estas, incluso en un contexto público.

Expresa el TEDH que, para determinar si el art. 8 CEDH es aplicable, procede examinar si las demandantes en cuestión eran objetivo de la medida de vigilancia, o si los datos personales que fueron procesados en un grado superior a lo que aquéllas podían haber previsto de forma razonable. Se explicó que la videovigilancia fue realizada durante 10 días, no pudiendo discutirse que varias demandantes no fueran objeto de la misma, ya que trabajaban detrás de las cajas, mientras que otras eran grabadas cuando pasaban por la zona. En cuanto a la previsión razonable, el supermercado es un lugar abierto al público y la grabación de la zona de cajas, donde se realizan los pagos de las compras, no tiene carácter íntimo o privado, por lo que las expectativas de protección de su vida privada eran limitadas indefectiblemente. Los trabajadores del supermercado, en general, habían sido informados de la colocación de otras cámaras, que enfocaban a la entrada y salida del establecimiento, por lo que la posibilidad de ser objeto de vigilancia era razonable, y considera el art. 8 CEDH aplicable. El TEDH observa que la medida de vigilancia denunciada por las demandantes se impuso por su empleador, una empresa privada, y por ello no puede estudiarse como una intrusión por parte del Estado; sin embargo, la responsabilidad de este puede verse implicada si los hechos denunciados emanan de su incapacidad para garantizar a los interesados el disfrute del derecho mencionado.

[10] Sentencia de la Gran Sala del Tribunal Europeo de Derechos Humanos, de 17 de octubre de 2019, asunto López Ribalda y otros contra España. Disponible en: https://hudoc.echr.coe.int/spa#{%22tabview%22:[%22translation%22],%22itemid%22:[%22001-197098%22]}. Consultada el 6 de febrero de 2020.

Las personas que habían visto las grabaciones realizadas de los 10 días mencionados fueron el gerente del supermercado, el representante legal de la empresa y el representante del sindicato de trabajadores, y no fueron usadas con otro fin que no fuese averiguar quiénes eran las personas que habían cometido los robos y habían ocasionado las pérdidas, para poder adoptar las medidas disciplinarias oportunas, y, en su caso, disponer de pruebas para posibles procedimientos contra ellos. Si bien la exigencia de transparencia y el derecho a la información eran de carácter fundamental, solo un requisito primordial referente a la protección de intereses públicos o privados significativos podría justificar la falta de información previa. En este caso, haber dado información sobre los hechos que se estaban sucediendo a cualquier empleado, podría haber frustrado el propósito de la vigilancia, impidiendo conocer a los autores de los hechos y no pudiendo recibir una compensación. Los tribunales laborales españoles consideraron en su día que no podía haberse empleado una medida menos lesiva para obtener la información y que existía proporcionalidad en su adopción. Si no hubiese existido, en términos generales, una mínima sospecha de apropiación indebida o cualquier otro acto ilícito por parte de los empleados, no hubiese sido legítima la instalación de las cámaras de videovigilancia, pero en este caso, dada la sospecha razonable, concreta, y la magnitud de las pérdidas, el TEDH considera que esto constituye una razón de peso que justifica lo anterior. Además, el robo pudo consistir en una acción concertada entre varios empleados, pues tales cantidades de dinero son complejas de sustraer por una sola persona, lo que genera una desconfianza generalizada en el entorno de trabajo. Por todo ello, el TEDH concluye y sostiene, por catorce votos contra tres, que no existe violación del derecho a la intimidad reconocido en el art. 8 del CEDH.

1.2 Derecho al secreto de las comunicaciones (18.3 CE)

El artículo 18.3 de la Constitución instituye un pilar fundamental en nuestra legislación, formando parte del ámbito de exclusión que cada persona elige frente a terceros y, lo que es más importante, frente a los poderes públicos. La posibilidad de que las comunicaciones que efectúa la persona investigada y las que recibe queden sometidas a que un tercero pueda escucharlas, *"por más que se trate de un agente de la autoridad debidamente habilitado por autorización judicial, convierte aquella diligencia en un verdadero instrumento de control de los poderes públicos frente a una de las más singulares manifestaciones de la privacidad"*. Por ello, la CE prohíbe las investigaciones

que tengan por objeto prevenir delitos futuros, porque el derecho fundamental que nos ocupa no puede limitarse sin considerar antes una base objetiva[11].

A su vez, el art. 82 de la LOPDPGDD proclama el derecho a la seguridad de las comunicaciones que los usuarios, mediante internet, emitan y reciban, siendo deber de los proveedores de estos servicios informar a aquéllos de sus derechos.

También está el caso de los ordenadores, que normalmente contendrán información relacionada con el derecho a la inviolabilidad de las comunicaciones, además de, por supuesto, afectar al derecho a la intimidad y protección de datos. Para acceder a aquélla, se habrá de contar con el consentimiento del afectado o, en su defecto, con autorización judicial[12]. Este dispositivo es un instrumento útil para la emisión o recepción de correos electrónicos, o mensajes a través de programas de mensajería instantánea, que lo que hacen es permitir la comunicación de forma libre entre personas. Los e-mails que son descargados desde el servidor correspondiente, leídos por el receptor y almacenados en la bandeja oportuna, se encontrarían fuera del ámbito de la inviolabilidad mencionada, siendo únicamente susceptible de protección por el derecho a la intimidad, por el hecho de ser acumulados en la memoria del terminal[13].

En cuanto a los teléfonos móviles, se dio un caso en que los agentes de la Policía Nacional hallaron un dispositivo en el lugar de la comisión de un delito, y accedieron a la agenda donde se encontraba simplemente el listado de contactos. En este caso el Tribunal Supremo consideró que no se vulneró el derecho al secreto de las comunicaciones, ya que en aquélla no se contienen datos sobre comunicaciones realizadas o recibidas, equiparándola a una agenda en formato físico, de papel. Ello hubiese sido al revés si hubiesen accedido al registro de llamadas. En cualquier caso, sí que se vulneró el derecho a la intimidad[14].

1.3 Derecho a la protección de datos (18.4 CE)

[11] STS 554/2019, de 13 de noviembre, FJ 1º.
[12] STS 528/2014, de 16 de junio, FJ 1º.
[13] STS 489/2018, de 23 de octubre, FJ 6º.
[14] Ibídem.

Las personas físicas, con el avance de los tiempos y la tecnología, necesitan un ámbito de protección respecto al tratamiento de sus datos personales, conforme al Preámbulo de la LOPDPGDD. La base que consolidó este derecho llegó con dos pronunciamientos clave del Tribunal Constitucional, que veremos a continuación.

En primer lugar, la Sentencia 290/2000[15] resuelve varios recursos de inconstitucionalidad del año 1993 interpuestos por el Consejo Ejecutivo de la Generalidad de Cataluña, el Defensor del Pueblo, el Parlamento de Cataluña y 56 Diputados del Grupo Parlamentario Popular contra distintos artículos de la LORTAD. Recoge pronunciamientos de gran interés sobre la naturaleza y labor de la Agencia de Protección de Datos y un voto particular mediante el que se reconoce un nuevo derecho fundamental, "el derecho a la libertad informática".

La razón de la que deriva el conflicto entre el Parlamento y el Consejo Ejecutivo de Cataluña son varios artículos de la LORTAD que se impugnaron, y está en que, según el art. 40 de esta, a las Comunidades Autónomas únicamente se les conceden facultades de ejecución de la propia ley referidas a ficheros automatizados de datos creados o gestionados por las propias CCAA en el ámbito de sus competencias[16], reservando en exclusiva la tutela administrativa de los ficheros de titularidad privada y los creados por la Administración Local a la Agencia de Protección de Datos, órgano de naturaleza estatal[17], para la mejor protección de los derechos (el art. 18.1 CE) frente al uso de la informática, como dispone el apartado 4 de ese mismo precepto[18].

El Tribunal Constitucional alude al origen de la propia LO para dar respuesta al conflicto; esta se dictó obedeciendo el mandato del art. 18.4 CE, y su fin es definir de una forma más concreta el uso que debe darse a la informática para proteger los datos personales, en cuanto forman parte del derecho fundamental a "la libertad informática". Es por ello que las facultades de información, inspección y sanción que se le atribuyen a la AEPD acerca de los ficheros de titularidad privada que se hallan en territorio autonómico, encuentran su lugar en el art. 18.4 CE, destinado a garantizar a los ciudadanos el compendio de potestades que integran el contenido de dicho derecho fundamental.

[15] Pleno. STC 290/2000, de 30 de noviembre (BOE núm. 4 de 4 de enero de 2001).
[16] Ibídem, FJ 2º.
[17] Ibídem, antecedente 1º.
[18] Ibídem.

El Tribunal Constitucional atribuye dichas facultades para la prevención de la violación de derechos fundamentales, *"Y dado que la garantía de estos derechos, así como la relativa a la igualdad de todos los españoles en su disfrute es el objetivo que guía la actuación de la Agencia de Protección de Datos, es claro que las funciones y potestades de este órgano han de ejercerse cualquiera que sea el lugar del territorio nacional donde se encuentren los ficheros automatizados conteniendo datos de carácter personal y sean quienes sean los responsables de tales ficheros"*[19].

El otro aspecto de interés a tratar sobre la Sentencia que venimos examinando, es el voto particular de dos Magistrados de dicho Tribunal, realizado por Don Manuel Jiménez de Parga y Cabrera, y al que se adhiere Don Rafael de Mendizábal Allende. Creen que, a la hora de redactar nuestro texto constitucional, *"se olvidó, o no quiso recogerse"*[20] una especie de cláusula abierta que coronase los derechos fundamentales, para que con el avance de los tiempos, fuera más sencillo introducir y recoger derechos modernos en nuestro ordenamiento jurídico, ya que estos están siendo creados por la jurisprudencia.

Consideran que el Tribunal debería haber reconocido en el fallo de forma explícita el derecho a la libertad informática y sostienen su apoyo a la creación de este nuevo derecho partiendo de la base del art. 10.1 CE, en el que residen todos los derechos inherentes a la dignidad de la persona y el libre desarrollo de la personalidad, así como el respeto a la ley y a los derechos de los demás. A juicio de los Magistrados, igualmente *"son preceptos que facilitan la configuración de la libertad informática los contenidos en los arts. 18.1 (derecho al honor, a la intimidad personal y familiar y a la propia imagen) y 20.1 (libertad de expresión y de información), entre otros, así como los Tratados y Acuerdos internacionales, en cuanto son guías de interpretación constitucional (art. 10.2 CE)"*[21].

Tomando como referencia el mencionado art. 10.1 CE, extraen las palabras *"fundamentos del orden político y de la paz social"*, que son clave, pues los entienden como principios constitucionales que rigen la interpretación de todo el ordenamiento, y

[19] Vid. Pleno. STC 290/2000… FJ 14º.
[20] Vid. Pleno. STC 290/2000… Voto particular, punto 1.
[21] Vid. Pleno. STC 290/2000… Voto particular, punto 2.

estiman que con ellos es posible extender y aplicar la tutela a un derecho tan importante como es el derecho a la libertad informática.

En segundo lugar, la Sentencia 292/2000[22] se manifiesta como resultado de los recursos que promovió el Defensor del Pueblo contra los artículos 21.1 y 24.1 y 2 de la Ley Orgánica 15/99, de 13 de diciembre, de Protección de Datos de Carácter Personal.

En ella encontramos una definición muy interesante: *"El derecho fundamental a la protección de datos persigue garantizar a esa persona el poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado"*[23], y esa protección *"no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por tercero pueda afectar a sus derechos sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 de la CE otorga, sino los datos de carácter personal"*[24]. El Tribunal trata de extender este derecho fundamental a los datos personales públicos, datos que puedan identificar su ideología, raza, sexo, economía, y que por el hecho de ser públicos o visibles deben igualmente atender al poder de disposición y control del interesado o afectado. Cualquier intento de privación al sujeto de disposición y control sobre sus datos constituirá una vulneración a su derecho de protección de los mismos[25].

Todo ello supone que la persona obtiene el poder de disponer, controlar y saber quién posee esos datos personales y para qué, de modo que el individuo pueda consentir qué datos personales puede proporcionar determinada persona a un tercero, el Estado o un particular, o qué datos puede recabar este tercero, pudiendo oponerse a esa posesión o uso. Ese consentimiento se precisa en la potestad sobre recogida, obtención, acceso y su posterior almacenamiento y tratamiento[26].

Podemos observar la diferencia entre el derecho a la intimidad y el derecho a la protección de datos; en el primero, se exige a terceros un deber de no intromisión en la

[22] Pleno. STC 292/2000, de 30 de noviembre (BOE núm. 4 de 4 de enero de 2001).
[23] Vid. Pleno. STC 292/2000…FJ 6º.
[24] Ibídem.
[25] Pleno. STC 11/1981, de 8 de abril (BOE núm. 99 de 25 de abril de 1981), FJ 8º.
[26] Vid. Pleno. STC 292/2000…FJ 7º.

esfera íntima de las personas, mientras que en el segundo, se añade también la concesión al titular de los datos de una serie de potestades que obligan a terceros a tareas jurídicas no acogidas en el derecho a la intimidad, como el derecho a saber y ser advertidos acerca del destino y uso que se va a dar a los datos y de su posible cesión, así como el derecho de acceso, rectificación y cancelación de los mismos.

Volviendo a los preceptos impugnados, hacen alusión a la cesión de datos que las Administraciones Públicas hacen entre ellas y las circunstancias en que aquélla se puede promover.

El Tribunal Constitucional falló en la Sentencia declarando contrario a la Constitución y nulo el apartado 1 del art. 21 de la LOPD, que establece que los datos personales almacenados por las Administraciones Públicas no serán transmitidos a otras, excepto *"cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso o"*; también hizo ese reconocimiento de nulidad e inconstitucionalidad respecto del apartado 1 del art. 24 LOPD, cuando la información al afectado *"impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas"* y *"o administrativas"*, y de todo su apartado 2.

Por ende, y salvo que la cesión de datos se lleve a cabo por una norma con rango de Ley, si no es necesario acudir a las excepciones generales del artículo 11.2 LOPD, ni a las específicas del precepto 21.1 y 2 LOPD, será ineludible recabar la autorización de la persona afectada cuyos datos se encuentren en el fichero, para que sea posible la cesión de los mismos entre las Administraciones Públicas. Además, el derecho de información que asiste a los interesados, reconocido en el artículo 5.1 y 2 LOPD, sólo podrá ser excluido por las Administraciones Públicas cuando la información pueda perturbar a la Defensa Nacional, a la seguridad pública, o por causa de una infracción penal[27].

[27] Disponible en: http://www.madrid.org/usupadron/legislacion/protdatos/protecciondatos.pdf, p. 7. Cul-sultada el 3 de febrero de 2020.

1.4 La prueba preconstituida[28]

En estos apartados a continuación, podremos ver el carácter atribuido por la jurisprudencia a las pruebas obtenidas a través de las cámaras de videovigilancia y de los dispositivos de geolocalización.

1.4.1 Cámaras de videovigilancia

La Ley Orgánica 4/1997, de 4 de agosto[29], por la que se regula la utilización de **videocámaras**, trajo como consecuencia el Real Decreto 596/1999[30], que desarrolló e incorporó la posibilidad de que las Fuerzas y Cuerpos de Seguridad del Estado (en adelante, FCSE) instalen cámaras de videovigilancia en lugares públicos, para ofrecer a los ciudadanos la máxima seguridad y prevenir la comisión de delitos, y poder tener registrados los que ocurran en este tipo de vía. Para ello, las FCSE necesitan una autorización previa de la Administración, que exige informe preceptivo y vinculante de la Comisión de Garantías de Videovigilancia[31], regulada en el Capítulo III del R.D. mencionado supra.

Por su parte, también hemos de tener en cuenta la LOPSC, que en su art. 22 permite a la Policía Judicial el uso de las videocámaras: *"La autoridad gubernativa y, en su caso, las fuerzas y cuerpos de seguridad podrán proceder a la grabación de personas, lugares u objetos mediante cámaras de videovigilancia fijas o móviles legalmente autorizadas"*, conforme a las normas vigentes en dicha materia. Lo mismo podemos observar en el art. 588 *quinquies a)* LECRIM. Si de las grabaciones resultaran filmados hechos que pudieran ser constitutivos de ilícitos penales, deberán incorporarse en forma de soporte magnético o electrónico al atestado, dirigiéndolo al Juez de guardia correspondiente con la mayor inmediatez posible y, en todo caso, en el plazo de 72 horas desde su grabación[32], en virtud del art. 7 de la L.O. 4/1997. A su vez, indica el mismo art.

[28] DÍAZ MARTÍNEZ, M.; GIMENO SENDRA, V.: *Derecho Procesal Penal (para policías y criminólogos).* Ed. Edisofer, Madrid, 2018. Pp. 324-326 y 331-333.
[29] Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos. «BOE» núm. 186, de 5 de agosto de 1997.
[30] Real Decreto 596/1999, de 16 de abril, por el que se aprueba el Reglamento de desarrollo y ejecución de la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos. «BOE» núm. 93, de 19 de abril de 1999.
[31] En virtud del art. 16.*a* del R.D. mencionado supra.
[32] STS 1220/2011, de 11 de noviembre, FJ 7º.

que, *"de no poder redactarse el atestado en tal plazo, se relatarán verbalmente los hechos a la autoridad judicial, o al Ministerio Fiscal, junto con la entrega de la grabación".* Ello servirá para formar o reforzar la "*notitia criminis*".

En cuanto al valor que tendrán los soportes magnéticos o electrónicos respecto del procedimiento, el Tribunal Supremo ha señalado que, al formar parte del atestado y constituir un documento público oficial sobre el que existe la posibilidad de examen de oficio, serán considerados **prueba preconstituida**. El mismo Tribunal ha diferenciado y aclarado el concepto: *"*s*u diferencia con la anticipada está en que en la preconstituida la práctica de la prueba no tiene lugar ante el Tribunal Juzgador sino ante el Juez de Instrucción, con lo cual la inmediación desaparece al menos como inmediación espacio temporal, y queda reducida a la percepción del soporte en que la prueba preconstituida se documente y refleje. A veces se le denomina prueba "anticipada en sentido impropio" para reservar el término de "preconstituida" a las diligencias sumariales de imposible repetición en el Juicio Oral por razón de su intrínseca naturaleza"*[33].

La jurisprudencia establece que *"las pruebas a valorar son las practicadas en el juicio oral y que solo excepcionalmente pueden incorporarse las diligencias llevadas a cabo en la fase de instrucción. Concretamente en relación con las pruebas preconstituidas, hemos señalado que solo cuando es imposible o muy difícil su práctica en el plenario, puede acudirse al visionado o a la lectura de la declaración sumarial. De manera, que la regla general es que, siempre que sea posible, la prueba debe practicarse en el juicio oral y que debe concurrir justificación suficiente para sustituirla por el visionado o la lectura de la preconstituida"*[34].

Existe un ámbito cuanto menos curioso y del que poco se habla aunque mucho se practica, y es aquel que ha derivado del ejercicio del periodismo de investigación, y es cuando se utiliza una cámara oculta en la que, no mediando consentimiento de su destinatario, se realizan determinadas grabaciones que, a veces, pueden llegar a ser constitutivas de ilícito penal. El Tribunal Constitucional ha expresado su rechazo a las mismas, por el menoscabo del derecho a la propia imagen, vida privada e intimidad, declarándola como una prueba de valoración vedada. Asimismo, *"la captación no sólo de la imagen sino también de la voz, intensifica la vulneración del derecho a la propia*

[33] STS 96/2009, de 10 de marzo, FJ 3º; STS 788/2017, de 7 de diciembre, FJ 4º.
[34] STS 427/2019, de 26 de septiembre, FJ 2º.

imagen mediante la captación no consentida de específicos rasgos distintivos de la persona que hacen más fácil su identificación"[35].

Expone que, a pesar de la posible notabilidad pública de la información que se intente alcanzar y difundir, la captación videográfica de imágenes no tolerada través del uso de cámaras ocultas *"para su posterior difusión, también inconsentida, en que aparezca plenamente identificado el afectado, no resulta necesaria ni adecuada, desde la perspectiva del derecho a la libertad de información [art. 20.1 d) CE], al existir, con carácter general, métodos de obtención de la información y, en su caso, una manera de difundirla en que no queden comprometidos y afectados otros derechos con rango y protección constitucional"*[36].

La cámara oculta no constituye un medio en sí mismo inconstitucional, salvo que se dé un conflicto entre derechos fundamentales, tales como la libertad de comunicar información veraz y socialmente relevante o el "*ius puniendi*" del Estado, casos en los que habrá que ponderar.

1.4.2 Dispositivos de geolocalización

La llegada del GPS y otros dispositivos de **localización** espacial ha conferido a la Policía Judicial una forma trascendental para conocer con precisión la ubicación de la persona investigada o sus medios de transporte u objetos. El Tribunal Supremo reconoce la validez del uso de balizas de geolocalización o radiotransmisores, ya que *"no vulnera el derecho fundamental al secreto de las comunicaciones o supone una inferencia excesiva sobre el derecho fundamental a la intimidad a los efectos de exigir un control jurisdiccional previo y una ponderación sobre dicha afectación constitucional. Para esta Sala Segunda Tribunal Supremo la ausencia de relevancia constitucional se deriva de que se trata de diligencias de investigación legitimas desde la función constitucional que tiene la policía judicial, sin que en su colocación se interfiera en su derecho fundamental que requeriría la intervención judicial"*[37].

[35] Sala Primera. STC 12/2012, de 30 de enero (BOE núm. 47 de 24 de febrero de 2012), FJ 5º.
[36] Sala Primera. STC 74/2012, de 16 de abril (BOE núm. 117 de 16 de mayo de 2012), FJ 2º.
[37] STS 798/2013, de 5 de noviembre, FJ 11º.

La geolocalización también puede llevarse a cabo mediante dispositivos telefónicos, cuyos datos se almacenan en el SITEL como en las compañías de telecomunicaciones, aunque en estas últimas el tiempo de conservación es limitado, solamente durante un año[38], lo cual facilita la ubicación e identificación en tiempo real de cada comunicación. A diferencia del SITEL, en las compañías la precisión no es exacta, sino que forma un perímetro que concretan las distintas antenas de telefonía.

El uso de estos dispositivos se regula en el art. 588 *quinquies b) de la LECRIM*. En el caso de que existan motivos de necesidad y proporcionalidad de la medida, el Juez se pronunciará de forma motivada, señalando el medio técnico a emplear, el objetivo de la medida y la persona o el bien que quedarán afectados, pues sobre ellos podrá colocarse el dispositivo. En caso de urgencia, la Policía Judicial situará el mismo, poniéndolo en conocimiento del Juez en el plazo de 24 horas, quien ratificará o rechazará la medida. Al mismo deberán entregarse los soportes originales o las copias electrónicas auténticas que compilen todos los datos obtenidos, cuando él lo solicite y en todo caso cuando termine la investigación.

Toda la información que custodie el Juzgado deberá ser destruida cuando recaiga sentencia absolutoria o sobreseimiento libre, o seguir preservada 5 años desde la ejecución de la pena o hubiere prescrito, en caso de sentencia condenatoria.

1.4.3. La prueba ilícita

En nuestro ordenamiento jurídico, el primer caso lo encontramos en una conocida Sentencia del Tribunal Constitucional de finales de 1984[39]. Fue plasmado más tarde en la Ley Orgánica del Poder Judicial, el art. 11.1 LOPJ, que señala que, de obtenerse pruebas que vulneren los derechos fundamentales, se considerarán ilícitas y carecerán de valor probatorio. La mayor labor de concreción la han realizado los Tribunales, especialmente el Constitucional, delimitando sus excepciones, matices, y aplicaciones. *"Es necesario ubicar con claridad el fundamento de regla de exclusión. Solo desde esa*

[38] STJUE de 8 de abril de 2014 de la Gran Sala: declara la invalidez de la Directiva 2006/24/CE en lo relativo al mantenimiento indiscriminado de datos.
[39] Sala Segunda. STC 114/1984, de 29 de noviembre (BOE núm. 305 de 21 de diciembre de 1984): respaldó la nulidad de toda prueba obtenida a través de un acto violatorio de derechos fundamentales, público o privado, pues el origen del menoscabo no hacía este menos intolerable.

premisa se puede lograr un desarrollo coherente", según el Magistrado Sr. Del Moral García. Entre la sanción al autor del delito y la protección de los derechos fundamentales, se ha elegido esto último *"frente a la sanción en todo caso y a toda costa de todos los responsables penales. Es una decisión de política criminal no ya correcta sino muy acertada",* afirma en su Voto Particular[40].

En cuanto al derecho a la prueba en el proceso penal y la posible indefensión que proceda de la denegación de la misma, el Tribunal Constitucional ha expuesto que no toda irregularidad u omisión en materia probatoria que se produzca en el proceso originará por sí misma una indefensión que sea legalmente destacable, ya que la garantía constitucional del art. 24.2 CE resguarda solo los casos en los que la prueba sea *"decisiva en términos de defensa, de modo que, de haberse practicado la prueba omitida o si se hubiese practicado correctamente la admitida, la resolución final del proceso hubiera podido ser distinta. Y también se afirma al respecto que el recurrente debe justificar la indefensión sufrida"*.

Dicha pretensión contiene una doble vertiente: en primer lugar, el recurrente ha de "demostrar la relación entre los hechos que se quisieron y no se pudieron probar y las pruebas inadmitidas o no practicadas"; y, en segundo lugar, debe *"argumentar el modo en que la admisión y la práctica de la prueba objeto de la controversia habrían podido tener una incidencia favorable a la estimación de sus pretensiones"*[41].

A este respecto, resulta paradigmática la Sentencia[42] del llamado caso Falciani, porque se detalla cuándo será ilícita dicha prueba. Los hechos son que Hervé Falciani, un ingeniero informático del banco "HSBC Private Bank" en Ginebra, copió datos de su empresa en los cuales se hallaban nombres de clientes de varios países de la Unión Europea, en la denominada Lista Falciani por las autoridades. Sobre aquellos clientes recaía una razonable probabilidad de que defraudaban a la Hacienda Pública de diversos países de la Unión Europea, encubriendo fondos que había consignados en aquella entidad financiera. La lista fue requisada en un registro que se realizó al domicilio del mis-

[40] STS 239/2014, de 1 de abril, Voto Particular del Magistrado Don Antonio del Moral García.
[41] Vid. STS 1220/2011… FJ 5º.
[42] STS 116/2017, de 23 de febrero.

mo. En la resolución, el Tribunal Supremo trata de discernir sobre la validez como prueba de aquella elaboración de Falciani.

El Tribunal no dudaba en justificar que Falciani no actuaba como *"pieza camuflada del Estado al servicio de la investigación penal"*[43], ya que en principio él buscaba obtener un rédito económico ofreciendo estos datos a otras entidades o servicios estatales, y pretendía a su vez denunciar la injusticia del sistema tributario. Consecuentemente, se le excluía de la aplicación del artículo 11 LOPJ, pues no buscaba pruebas con el objeto, directo o indirecto, de hacerlas valer en un proceso penal.

Además, cuando Falciani se apropió ilícitamente de la información, no lo hizo como *"agente al servicio de los poderes públicos españoles interesados en el castigo de los evasores fiscales",* sino que lo hizo como particular. El Tribunal se centra mucho en hacer esta distinción entre particular y funcionario a la hora de abordar el menoscabo del derecho fundamental, como en el caso de las grabaciones realizadas por individuos que no ejercen un cargo público, de las cuales discutiremos más tarde. La finalidad disuasoria que es el punto de inicio para excluir la prueba ilícita no alcanzó a Falciani, que únicamente percibía en esos datos apropiados un negocio lucrativo[44].

En mi opinión, las personas físicas y jurídicas protagonistas de la extensa Lista de nombres han visto vulnerado su derecho a la intimidad, así como el banco donde estos clientes han depositado su confianza. La distinción entre funcionario y particular a mi juicio es irrelevante, porque los derechos fundamentales son prioritarios en cualquier caso, y, si eso no es así, los Poderes Públicos podrían utilizar este precedente de forma indiscriminada.

Acudiendo al Tribunal Supremo, encontramos dos sentencias clave. En la primera, una madre descubre que en el ordenador que usa toda la familia hay imágenes pornográficas del padre realizando actos depravados a su hija menor de edad. El padre, acusado, alega que la contraseña era conocida por todos ellos. Por un lado, el hecho del uso compartido supone un desafío probatorio en el sentido de acreditar la autoría de un hecho delictivo que se ha servido del uso de las nuevas tecnologías; por otro lado, la

[43] Vid. STS 116/2017… FJ 7º.
[44] Vid. STS 116/2017... FJ 8º.

utilización de una contraseña común hace que la vulneración del derecho a la intimidad sea más compleja de sostener ya que el titular del mismo amplía el entorno digital y se minimiza el ámbito de exclusión frente al resto de su familia. El acusado, al incluir dichas imágenes en un dispositivo de almacenamiento del cual hace uso la familia al completo, es consciente de que los límites entre lo íntimo y la posibilidad de conocimiento de terceros se desdibujan. La madre entregó en comisaría el ordenador y la memoria flash en la que se encontraban las imágenes de los abusos, tratándose de una prueba proporcionada y que no esquiva las garantías del sistema constitucional[45].

En definitiva, deben respetarse los criterios señalados por la jurisprudencia para no transgredir los derechos fundamentales mencionados, pues ello puede ocasionar la invalidez de la prueba obtenida, y, si es la única prueba disponible, la persona investigada puede quedar impune por imposibilidad de demostrar los hechos.

[45] STS 287/2017, de 19 de abril, FJ 2º.

CAPÍTULO II: ANTECEDENTES LEGISLATIVOS

El 6 de diciembre de 2015 entró en vigor la reforma de la LECRIM, llevada a cabo por la LOMLECRIM, terminando así un extenso período de vacío normativo en lo concerniente a las garantías que, ante el rápido avance de la tecnología en la persecución de los delitos, necesitaba de una regulación urgente. A pesar de ello, la nueva normativa ha generado múltiples dudas en cuanto a su aplicación, y, por esa razón, el 22 de marzo de 2019, el BOE publica cinco Circulares de la Fiscalía General del Estado que tratan de ilustrar al respecto.

En la jurisprudencia anterior a estos avances normativos ya se ponía de manifiesto la necesidad de afrontar una reforma legislativa que regulase las concretas medidas de investigación que son necesarias para el esclarecimiento de los delitos y cuyos vestigios o pruebas se contienen en los dispositivos tecnológicos, al ser *"raquítica e insuficiente"*[46] la regulación legal contenida, por ejemplo, en el art. 579 LECRIM, según señalaba el Tribunal Supremo. En la misma se declara la inexistencia de habilitación legal para llevar a cabo determinadas injerencias, pese a que éstas cuentan con autorización judicial otorgada mediante auto acordando *"artificios técnicos de escucha, grabación de sonido e imagen"*[47].

También se hicieron eco de esta situación otras resoluciones, estableciendo que, en la fase de investigación penal, la ponderación de los motivos que explican el sacrificio de los derechos, por ejemplo, del usuario de un ordenador, como titular de los mismos, ha de realizarse teniendo en cuenta que los datos que se acumulan en aquel terminal tienen abundantes utilidades. Se opta por el reconocimiento procesal de todos los derechos fundamentales de los arts. 18.1, 18.3 y 18.4 CE, no de una forma individualizada, sino que se prefiere denominar "el derecho al entorno virtual"[48], es decir, es imposible diferenciar cada uno de los derechos en el soporte tecnológico que los contiene, por lo que se opta por proteger dicho entorno de una forma similar a la protección de la vivienda; en el entorno virtual *"se integraría, sin perder su genuina sustantividad como manifestación de derechos constitucionales de nomen iuris propio, toda la información*

[46] STC 157/2014, de 5 de marzo, FJ 2º.
[47] Sala Segunda. STC 145/2014, de 22 de septiembre (BOE núm. 261 de 28 de octubre de 2014), FJ 1º.
[48] STS 342/2013, de 17 de abril, FJ 8º; STS 587/2014, de 18 de julio, FJ 5º.

en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos". Ello incita a la necesidad de proporcionar una protección jurisdiccional frente a la necesidad del Estado de invadir, en su labor de investigación y condena de los delitos, ese entorno digital. En esta materia no se pueden interpretar los términos de la autorización que se otorgue de forma extensiva ni elástica, pues nuestro ordenamiento jurídico no acoge autorizaciones tácitas, *"ni mandamientos de intromisión en el espacio de exclusión que definen los derechos fundamentales que no estén dibujados con la suficiencia e indispensable claridad"*[49].

Como pone de manifiesto MESTRE DELGADO[50] al analizar la STS 85/2013, de 4 de febrero, la ausencia de una regulación normativa clara, "defiere al ámbito de lo opinable las decisiones judiciales más extremas que puedan adoptarse en una materia tan sensible", ya que incide plenamente en nuestros derechos fundamentales, en este caso, en todos aquellos ligados a la privacidad e intimidad.

[49] Vid. STS 342/2013… FJ 8º.
[50] MESTRE DELGADO, E.: *La intimidad devaluada frente a la investigación de delitos*, Diario la Ley 2808, de 17 de mayo de 2013.

CAPÍTULO III: LA REGULACIÓN DE LA REFORMA EFECTUADA POR LA LEY ORGÁNICA 13/2015 Y LOS ASPECTOS COMUNES DE LA NUEVA REGULACIÓN

La LOMLECRIM adapta el lenguaje de la LECRIM a los tiempos actuales, prescindiendo de ciertas expresiones utilizadas de modo indistinto en la ley sin rigor conceptual; en el caso de la palabra "investigado", para identificar a la persona que se encuentra bajo investigación por su relación con un delito, mientras que con el término "encausado" se designa a aquella persona a quien la autoridad judicial, una vez haya finalizado la instrucción de la causa, se atribuye formalmente haber participado en la comisión de un determinado hecho delictivo. A su vez, esta LO se aplica a los procedimientos penales incoados con posterioridad a su entrada en vigor, y también a las diligencias policiales y fiscales, resoluciones y actuaciones judiciales dictadas en procedimientos penales en tramitación, según la Disposición Transitoria Única LOMLECRIM.

Por un lado, la LOMLECRIM transpone al ordenamiento jurídico interno la Directiva 2013/48/UE del Parlamento Europeo y del Consejo, de 22 de octubre de 2013, acerca del derecho a la asistencia de letrado en los procesos penales y en los relativos a la orden de detención europea, y sobre el hecho de informar a un tercero cuando se produce la privación de libertad y a comunicarse con terceros y con autoridades consulares durante la privación de libertad.

Por otro lado, adecúa la legislación a nuevas formas de comisión de delitos derivadas del uso de las nuevas tecnologías, modificándose el artículo 579 LECRIM, donde el Juez puede acordar la detención de la correspondencia privada, postal y telegráfica que la persona investigada remita o reciba, así como su apertura o examen, y nuevo artículo 579 *bis*, que indica que el resultado de lo anterior puede ser utilizado como medio de investigación o prueba en otro proceso penal; así como la inclusión de nuevas medidas de investigación tecnológica en los Capítulos V a VII del Título VIII del Libro II de la LECRIM. El Capítulo V dedicado a la interceptación de las comunicaciones telefónicas y telemáticas, el Capítulo VI a la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos y el **Capítulo VII a la utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización. Este último apartado constituye la razón de ser de este trabajo, y será mi ob-**

jeto de análisis. A continuación, se expondrán estas medidas, que se encuentran reguladas en el Capítulo IV del Título VIII del Libro II, introducido por el apartado trece del art. único LOMLECRIM.

3.1 Principios rectores [588 *bis a*)]

En principio, la adopción de las medidas podrá acordarse durante la instrucción de la causa siempre que exista autorización del Juez, y que esta se dicte conforme a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida.

El principio de especialidad supone que la medida correspondiente deberá tener por objeto el esclarecimiento de un delito concreto, no pudiendo permitirse aquellas que intenten prevenir hechos punibles que carezcan de un fundamento objetivo. Si de la adopción de la misma se produce como consecuencia el descubrimiento casual de una información que puede ser útil en otro procedimiento distinto, en virtud del art. 588 *bis i)* LECRIM, hay que acudir a lo dispuesto en el art. 579 *bis* LECRIM, de manera que habrá de expedirse un testimonio de los particulares necesarios para acreditar la legitimidad de la injerencia, a los efectos de ser incorporado al procedimiento por delito diferente contra la persona investigada.

El principio de idoneidad del art. 588 *bis a).3* de la LECRIM será útil para concretar el ámbito objetivo y subjetivo, así como la duración de la medida; respecto al primero, será concerniente a la autorización concreta que dicte el Juez que la acuerda; respecto al segundo, el art. 588 *bis h)* afirma que la medida se puede acordar incluso cuando afecte a terceros, siempre y cuando se den las condiciones establecidas en las disposiciones específicas de cada una de ellas. El juicio de adecuación posee el estatus de criterio negativo, es decir, mediante él se puede identificar de forma más sencilla qué medios no son idóneos para conseguir el fin legítimo pretendido; por ello, no determinará todos los medios aptos, sino que únicamente excluirá los que no lo son, según ZOCO ZABALA[51].

[51] ZOCO ZABALA, C.: *Nuevas tecnologías…,* op cit., pp. 133-134.

En virtud de los principios de excepcionalidad y necesidad[52], solo cabrá acordar la medida cuando no existan otras alternativas menos gravosas para los derechos fundamentales de la persona investigada o cuando el hallazgo *"o la comprobación del hecho investigado, la determinación de su autor o autores, la averiguación de su paradero, o la localización de los efectos del delito se vea gravemente dificultada"* si no se acude esta medida, alude el art. 588 *bis a).4* LECRIM. El objetivo es la menor intromisión posible en los derechos reconocidos en el CEDH.

Por último, se deduce del art. 588 *bis a).5* LECRIM que la medida será conforme al principio de proporcionalidad cuando haya sido tomada teniendo en cuenta que el sacrificio de los derechos e intereses afectados no sea superior al beneficio de adoptarla y cuando el juicio de la delimitación sea proporcional a la trascendencia del fin perseguido.

3.2 Solicitud y autorización judicial de la medida de investigación tecnológica

El art. 588 *bis b)* establece que el Juez de instrucción es el que acordará las medidas, de oficio o a instancia del Ministerio Fiscal o la Policía Judicial. Después de analizar la petición, el Juez deberá autorizar o denegar la medida a través de un auto motivado[53], tras haber oído al Ministerio Fiscal, según el art. 588 *bis c).*

3.3 Duración de la medida, prórroga y cese

En cuanto a la duración, conforme al art. 588 *bis e),* cada medida tendrá concretada la suya, no pudiendo exceder del tiempo imprescindible para el esclarecimiento de los hechos, y podrá haber prórrogas cuando persistan las causas que la ocasionaron, dirigiéndose la solicitud por el Ministerio Fiscal o la Policía Judicial al Juez competente, señala el art. 588 *bis f).* El Juez resolverá mediante auto motivado si la concede en el plazo de los dos días siguientes a la presentación de aquélla. Una vez concedida, comenzará a computarse desde la fecha de expiración del plazo de la medida acordada.

[52] GARCIMARTÍN MONTERO, R.: *Los medios de investigación tecnológica en el proceso penal,* Cizur Menor (Navarra), 2018, p. 34.
[53] TOMÉ GARCIA, J.A.: *Curso de Derecho Procesal Penal,* Madrid, 2016, pp. 249 y ss.

En virtud del art. 588 bis j), el Juez acordará el cese de la medida cuando haya transcurrido el tiempo por el que se concedió la misma sin que se haya acordado prórroga, cuando se haya consumado esta, o bien cuando hayan desaparecido las circunstancias que justificaron la adopción de la medida, o cuando sea evidente que mediante la misma no se están cumpliendo las expectativas sobre los resultados.

3.4 Control judicial y secreto

El art. 588 *bis g)* determina que la Policía Judicial será la encargada de comunicar al Juez de instrucción el desarrollo y los resultados de la medida, en la forma y con la regularidad que el mismo fije, y siempre que exista causa que ponga fin a la misma.

Mientras dura la medida, los resultados que se vayan recopilando se incorporan al proceso a través de los soportes convenientes, como grabaciones o transcripciones, aunque se mantendrán en una pieza separada y secreta para las partes, con el propósito de no perjudicar el resultado de la investigación. Una vez acordado el cese de la medida, se alzará el secreto y se facilitará a las partes copia de los soportes, según señala el art. 588 *ter i)* de la LECRIM.

CAPÍTULO IV: LA UTILIZACIÓN DE DISPOSITIVOS TÉCNICOS DE CAPTACIÓN DE LA IMAGEN, DE SEGUIMIENTO Y DE LOCALIZACIÓN

En las medidas descritas en el título entran en juego los derechos fundamentales al secreto de las comunicaciones, a la propia imagen, la intimidad, o la inviolabilidad del domicilio, entre otros. Si es necesario el sacrificio de alguno o varios de ellos, se requerirá una motivación mayor para poder proceder al uso de las medidas.

Localizamos un antecedente a esta nueva legislación en la STC 145/2014, que concluye que las grabaciones en dependencias policiales resultaron contrarias al art. 18.3 CE, deviniendo nula la prueba obtenida por ese cauce por falta de habilitación legal, a pesar de tener autorización judicial para llevarlas a cabo[54].

La STS 513/2010 no consideraba racional que una conversación telefónica pudiera ser legítimamente intervenida por el Juez y, por el contrario, una conversación mantenida entre dos individuos en un recinto cerrado no pueda serlo. Por ello, y en relación a un caso en un centro penitenciario, dictó una resolución ese mismo año, razonando que, si la legislación penitenciaria autoriza al director de aquél a grabar conversaciones entre detenidos en los calabozos policiales, mayor permisibilidad deberá aplicarse al Juez de instrucción[55].

Finalmente, la exigencia de regulación de estas medidas que mencionamos en el Capítulo II se encuentra detallada en la *Circular 4/2019, de 6 de marzo, de la Fiscalía General del Estado, sobre utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización,* que veremos a continuación de forma extensa.

4.1 Utilización de dispositivos técnicos de captación de imagen

Esta medida se dirige a la exploración de comportamientos delictivos en la instrucción del procedimiento penal, limitando su uso a las actuaciones de la Policía Judicial tendentes a la elaboración del juicio, dando la posibilidad de investigar y constatar

[54] Sala Segunda. STC 145/2014, de 22 de septiembre (BOE núm. 261 de 28 de octubre de 2014), FJ 7º.
[55] STS 513/2010, de 2 junio, FJ 4º.

la comisión del delito y la consecuente culpabilidad de los autores, en virtud del artículo 299 de la LECR.

Si no nos encontramos dentro de la investigación de estos comportamientos, la captación de imágenes ajenas, aun en lugares públicos, puede producir para el sujeto que ha sido grabado una intromisión en su esfera del derecho a la intimidad y propia imagen[56], no legitimada[57] por no estar en la instrucción de un procedimiento. Otro caso que queda fuera del ámbito de investigación, y cuya finalidad es distinta de todo la anterior, es el del mantenimiento de la seguridad y prevención de delitos en lugares públicos, que permite la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad para grabar sonidos e imágenes[58]. Esta labor de prevención posibilita la incorporación a un procedimiento penal de aquellas grabaciones que puedan llegar a constituir prueba o indicio de delito; en ese caso, se dispone que de forma inmediata o en 72 horas desde la grabación, la cinta o soporte original de las imágenes y sonidos deberán ser puestas en su integridad a disposición judicial por las Fuerzas y Cuerpos de Seguridad[59]. En caso de no poder realizarse el correspondiente atestado en el plazo señalado, los hechos serán relatados verbalmente junto a la entrega de la grabación ante la autoridad judicial o el Ministerio Fiscal.

Tampoco forman parte de este ámbito de aplicación las grabaciones realizadas por vigilantes de seguridad o guardas rurales[60], que en este caso no podrán tomar imágenes y sonidos de vías y espacios públicos; cuando dichas grabaciones puedan relacionarse con posibles ilícitos penales o perturbar la seguridad ciudadana, serán aportadas a las Fuerzas y Cuerpos de Seguridad competentes, de *motu proprio* o petición de estas, cuidando y respetando la conservación y custodia *"para su válida aportación como evidencia o prueba en investigaciones policiales o judiciales"*[61].

En cuanto a los particulares, la Ley de Enjuiciamiento Criminal no les aplica el artículo 588 *quinquies a)* porque no son llevadas a cabo por la Policía Judicial, pero tampoco les disuade de realizar grabaciones videográficas, por lo que, si aprecian que se

[56] Art. 7 LO 1/1982, de 5 mayo.
[57] Legitimación por art. 2.2 LO 1/1982, de 5 de mayo.
[58] Art. 1 LO 4/1997, de 4 agosto.
[59] Art. 7 LO 4/1997, de 4 agosto.
[60] Ley 5/2014, de 4 de abril. Art 42.
[61] Art 42 Ley 5/2014, de 4 abril.

están produciendo hechos que pudieran considerarse delictivos o que pudieran aportar información en una investigación penal. Ello únicamente es válido si se trata de una grabación a un particular puntual o casual, pues la grabación preordenada es competencia exclusiva de la Policía Judicial[62].

4.1.1 Captación de imágenes en lugares o espacios públicos, en virtud del artículo *588 quinquies a)*. Conceptos

El elemento esencial para poder aplicar la medida es que la persona a la que se está investigando, cuyas imágenes se pretende captar, se encuentre en lugar o espacio público, y según el art. 22.2 LOPDPGDD, en la medida en que resulte imprescindible para la seguridad de personas y bienes, así como de sus instalaciones; es necesario establecer, por lo tanto, la naturaleza pública o privada de este, para lo cual se habrá de atender la perspectiva de la privacidad y el ejercicio del derecho a la intimidad.

Así las cosas, el derecho a la intimidad regulado en la Ley Orgánica 1/1982 tiene como límite la privacidad, por ser un ámbito reservado frente *"a la acción y el conocimiento de los demás"*, excluyendo también a los *"poderes públicos o simples particulares"*[63], indispensable para que cada persona pueda desenvolver su vida con una calidad mínima.

Por lo tanto, frente a la lectura del art. *588 quinquies a),* deberá entenderse por públicos aquellos espacios donde la persona investigada no pueda ejercitar su derecho a la intimidad, ni tenga derecho de exclusión sobre estos lugares; en cambio, por privados serán el domicilio, vestuarios de gimnasio o supermercado, el cuarto de baño…aquí sí puede excluirse el acceso de terceros, por existir el límite de la privacidad mencionado.

4.1.1.2 Casos prácticos

Un caso que puede plantearse de forma automática es qué sucede cuando se graban imágenes del interior de un domicilio desde fuera. La única vía que ha estado dando una solución a esta cuestión ha sido la jurisprudencia del Tribunal Supremo; establecía

[62] STS 968/1998, de 17 julio, FJ 1º.
[63] STC 134/1999, de 15 julio, FJ 2º.

que la respuesta podía variar según si para realizar la grabación se valían de artificios técnicos o no. Éstos son instrumentos que refuerzan la capacidad normal de observación. Si se utilizan, el TS entiende que se produce una invasión en la intimidad de los sujetos grabados, por lo que este acto requeriría autorización judicial[64], y, si no se utilizan, no hay que vencer ningún tipo de barrera natural, y no se requiere dicha intervención[65].

Como ejemplo paradigmático tenemos el de unos agentes de la policía que realizaron observaciones del interior de la vivienda del principal acusado, situada en el décimo piso de un edificio de viviendas, desde un inmueble próximo, haciendo uso para ello de unos prismáticos[66]. La sentencia que analiza el caso proviene del Tribunal Supremo, y entiende que tanto frente al acto de intrusión no consentido en el domicilio, como a la contemplación furtiva de lo que sucede en su interior, se encuentra la tutela del artículo 18.2 CE, referente a la inviolabilidad del domicilio, siempre y cuando estas actuaciones hayan sido realizadas con *"artilugios técnicos de grabación o aproximación de imágenes"*[67], que permitan aumentar éstas y pasar la "barrera natural" entre la persona que observa, que cuenta con ventaja, y la que es observada. El hecho de que unas persianas estén subidas o que unas cortinas no estén corridas por el inquilino, no implica que autorice de forma implícita a contemplar, como ya se mencionó, el interior del inmueble, donde lleva a cabo su vida, pues ello produciría un perjuicio al derecho contenido en el artículo 18.2 de la CE.

El artículo *588 quater a)* impone la necesidad de obtener autorización judicial para la utilización de dispositivos electrónicos orientados a la grabación de imágenes; aunque no permitan esta acción, este podría ser el caso de unos prismáticos, si bien la legislación no los contempla específicamente. En el presente caso, al haberse realizado las observaciones del interior de la vivienda del acusado, desde un inmueble próximo, utilizando el artilugio mencionado, no se verifica *"la existencia de fin constitucionalmente legítimo que, por razones de urgencia, permitiera sacrificar la intimidad del sospechoso"*[68]. Existió una *"intromisión en el contenido material del derecho a la inviolabilidad*

[64] STS 354/2003, de 13 marzo, FJ 2º; STS 329/2016, de 20 abril, FJ 2º.
[65] STS 453/1997, de 15 abril, FJ 1º.
[66] STS 329/2016, de 20 abril, FJ 2º
[67] Ibídem.
[68] Ídem.

del domicilio"[69], que supuso la nulidad de la principal prueba de cargo, como es la observación que los agentes llevaron a cabo, y la correspondiente absolución de los acusados. Como podemos comprobar, hay que tener muy en cuenta y seguir criterios legales al proceder de forma estricta, pues la trascendencia de perder una prueba así supone perder toda posibilidad de condena.

La conclusión de todo ello es que, en un principio, la captación de imágenes no exige autorización judicial cuando se realiza con respeto al derecho a la intimidad de la persona investigada y en espacios abiertos y de uso público[70], pero, en el momento en que esta acción comprometa este derecho, para poder adoptar la medida se habrá de aplicar extensivamente el artículo 588 *quater a)*, es decir, será requisito tener autorización judicial. Por el contrario, cuando esa captación no implique adentrarse en la intimidad del sujeto y no sea necesaria la utilización de dispositivos técnicos específicos, deberá aplicarse el 588 *quinquies a).*

4.1.2 Principios Rectores

Se establece en el art. *588 bis a)* que mientras se esté instruyendo la causa se puede disponer la aplicación de alguna medida de investigación contenida el Capítulo IV del Título VIII del Libro II de la LECRIM, previa autorización judicial sometida a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida.

En el contexto en que nos encontramos, de adopción de una medida para la captación de imágenes en lugar o espacio público, no es necesaria la solicitud de autorización judicial del art. 588 *bis b*) en principio, como ya fue mencionado, si bien cuando invada la privacidad de la persona investigada será necesaria y debería respetar los principios aludidos *ut supra*. Tampoco serían aplicables en un primer momento la resolución judicial del art. 588 *bis c*) o la duración del art. 588 *bis e*) y prórroga de la medida del art. 588 *bis f*), aunque todas ellas sean disposiciones comunes a todas las medidas reflejadas en el Capítulo IV, Título VIII, Libro II. Lo que ahora se plantea es si será

[69] Ídem, FJ 3º.
[70] STS 990/2016, de 12 enero 2017, FJ 12º.

indispensable que la diligencia de investigación en sí misma se sujete a dichos principios.

Volviendo al art. 588 *quinquies a),* su adopción exige que la medida sea indispensable para proporcionar la identificación de la persona investigada, para localizar las herramientas o instrumentos del delito u obtener datos que tengan relevancia para aclarar los hechos. Estas pretensiones concretas emanan del principio de necesidad y, por tanto, obligarán al Juez Instructor a apreciar su concurrencia cuando se haya de anexar el resultado de la medida al procedimiento.

La consecuencia que se desprende de todo ello es que la captación de imágenes en lugares o espacios públicos posee un régimen distinto respectos de las otras diligencias de investigación tecnológica; mientras que en estas otras el Juez deberá valorar previamente los principios respecto de la medida, en la que nos ocupa, será primero practicada por la Policía Judicial, siendo posterior el análisis de la concurrencia de los principios rectores por el Juez en el caso concreto.

Como indica GARCIMARTÍN MONTERO[71], uno de los mayores problemas que plantea el uso de la captación de imágenes es la ausencia de una norma sobre la duración de la medida, lo que planteará problemas de interpretación.

4.1.3 Disposiciones comunes

Serán aplicables a todas las medidas de investigación tecnológica los preceptos relacionados con el secreto, control de la medida, utilización de la información obtenida en procedimientos distintos y descubrimientos casuales, y destrucción de registros, los cuales serán descritos a continuación.

4.1.3.1 Secreto, artículo 588 *bis d)*

Supone que en los casos en los que la captación de imágenes vaya a ser una medida mantenida durante un tiempo, aunque no se convenga de forma expresa el secreto

[71] GARCIMARTÍN MONTERO, R..: *Los medios de investigación tecnológicos en el proceso penal, op. cit*, P. 109.

del litigio, la solicitud de esta y los actos ulteriores que se realicen, serán llevados a cabo a través de una pieza separada y secreta, para no malograr su eficacia. Por el contrario, cuando la grabación sea puntual y no haya necesidad de continuar aplicando la medida, no habrá motivos para conservar de forma secreta la investigación.

4.1.3.2 Utilización de la información obtenida en procedimiento distinto y descubrimientos casuales, artículo 588 *bis i)*

Este artículo nos remite al art. 579 bis, que se aplica a su vez a la detención y apertura de la correspondencia escrita y telegráfica. Señala que, al producirse un descubrimiento casual cuando se están captando imágenes, al no haber autorización judicial, la forma de proceder para comunicarlo al otro procedimiento es mediante la remisión del testimonio del resultado de la captación y del oficio policial que acompañe su presentación en el Juzgado. También habrán de añadirse, entre los antecedentes imprescindibles, la solicitud que inició la adopción, la resolución del Juez que la acordó, y todas las peticiones con sus correspondientes resoluciones de prórroga recaídas en el procedimiento de origen[72].

El hallazgo casual o elemento probatorio novedoso *"que no está inicialmente abarcado por el principio de especialidad, puede ser utilizado en el propio o distinto procedimiento, bien por tratarse de un delito flagrante o bien por razones de conexidad procesal, siempre que, advertido el hallazgo, el juez resuelva expresamente continuar con la investigación para el esclarecimiento de ese nuevo delito, ante la existencia de razones basadas en los principios de proporcionalidad e idoneidad. El hallazgo no solamente se proyecta hacia el futuro […], sino también puede producirse hacia el pasado".* Tal línea de investigación ha de ser mostrada al Juez, para que, *"valorando los intereses en juego, acceda a su incorporación al proceso, conjugando un elemental principio de proporcionalidad. Se trata, en suma, de aquellos descubrimientos casuales que pueden aportar luz para el esclarecimiento de los hechos, de carácter novedoso (puesto que permanecían ocultos), y que han de ser investigados, con tal que la autoridad judicial pondere su importancia, salvaguarde el principio de especialidad, y justifique su necesidad y proporcionalidad"*[73].

[72] ZOCO ZABALA, C.: *Nuevas tecnologías…. Op. cit.,* P. 183.
[73] STS 777/2012, de 17 de octubre, FJ 2º.

4.1.3.3 Destrucción de registros, artículo 588 *bis k)*

La captación de imágenes en lugares o espacios públicos crea registros con un propósito en el procedimiento, por lo que, una vez cumplido, han de ser destruidos, pues según el Preámbulo de la LOMLECRIM, *"se pretende con ello evitar toda difusión de un material que, por su propio contenido, podría dañar de forma irreparable la intimidad del afectado"*[74].

En este apartado hemos de acudir a la *Circular 1/2019, de 6 de marzo, de la Fiscalía General del Estado, sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológicas en la Ley de Enjuiciamiento Criminal,* que alude también a esta disposición, incidiendo en que la cesación de la captación está sujeta a tres motivos, reflejados a su vez en el art. 588 *bis j),* aunque este parece estar previsto para una medida continuada y no puntual; estos son que se desvanezcan los principios rectores que justificaron la adopción de la medida, que sea indudable que no se logran los resultados pretendidos con la medida, o que haya pasado el plazo originalmente fijado para su ejecución.

Debe tenerse en cuenta que, aunque inicialmente la medida no dé resultados, no significa que no sea apta, y que siempre que continúen los motivos que justificaron la adopción y si se conjetura que podrá proyectar datos relevantes posteriormente, el principio de idoneidad para con el fin perdurará para el mantenimiento de la medida.

El art. 588 *bis k)* diferencia entre registros originales y copias para abordar la destrucción, que apunta solamente al dónde están y quién las tiene, pero no a qué calidad posee o su naturaleza.

Los originales pueden figurar en sistemas electrónicos como el SITEL[75] y estarán bajo el control de unidades policiales. Una vez finalice el procedimiento a través de

[74] Preámbulo de la *Ley Orgánica 13/2015 de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica,* p. 5., Vid: ARMENTA DEU, T.: *Lecciones de Derecho procesal penal,* Madrid, 2016, p. 134, la medida se introduce para evitar toda posible difusión posterior e impedir el daño irreversible que se puede producir en la intimidad del afectado por la medida.

[75] El sistema SITEL es un sistema de escuchas telefónicas del Ministerio de Interior de España que es utilizado por la Policía Nacional, la Guardia Civil y el Servicio de Vigilancia Aduanera. Este sistema

la correspondiente sentencia, y esta devenga firme, o cuando en el mismo se dicte auto de sobreseimiento libre, y haya adquirido firmeza, será obligatorio destruir los registros originales.

Las copias, en cambio, son almacenadas en el Juzgado custodiadas por el Letrado de la Administración de Justicia. Si en el procedimiento ha recaído sentencia condenatoria, deberán transcurrir 5 años desde la ejecución de la pena, o lo que es lo mismo, desde el auto que acuerde su extinción definitiva. Si hay sentencia absolutoria firme o se ha decretado el sobreseimiento libre, podrán destruirse las copias; en caso contrario, habrá que esperar a que el delito o la pena prescriban. Si se produce esto último, será imprescindible que así se manifieste por una resolución judicial.

En el caso de que se quieran revisar las pruebas, y para ello se interponga algún recurso como puede ser el extraordinario de revisión, el de amparo o ante el Tribunal Europeo de Derechos Humanos, la autoridad juzgadora puede encontrarse con el impedimento de que los registros se hayan destruido, si la resolución judicial ha adquirido firmeza y han pasado 5 años desde su ejecución. En aras de protección de esta circunstancia, y en virtud del apartado segundo del art. 588 *bis k)*, el Tribunal puede pactar que se preserven los registros. Esto último se concibe como excepción a la regla general, siendo una potestad discrecional del Tribunal, por lo que en consecuencia requiere una motivación intensificada; tal y como podemos apreciar en la STS n.º 854/2013, de 30 de octubre, *«el fundamento de extender el deber reforzado de motivación (…) se encuentra en que el margen de discrecionalidad del que legalmente goza el Juez no constituye por sí mismo justificación suficiente de la decisión finalmente adoptada, sino que, por el contrario, el ejercicio de dicha facultad viene condicionado estrechamente por la exigencia de que la resolución esté motivada, pues sólo así puede procederse a su control posterior en evitación de toda arbitrariedad»*. Ha de tenerse en cuenta, además, que existirán numerosas copias de los registros fuera del Juzgado, bajo dominio de la Fisca-

aparece regulado en el *Real Decreto 424/2005, de 15 de abril, por el que se aprobó el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas y el servicio universal y la protección de los usuarios*. Disponible en: https://www.iberley.es/temas/sistema-sitel-interceptacion-comunicaciones-telefonicas-telematicas-proceso-penal-63164, Consultada el 14 de enero de 2020. El *SITEL "cumple con todas las exigencias y garantías propias de esta clase de diligencias de investigación y probatorias que cuentan con una previa autorización judicial para su práctica"*, en virtud de la STS 753/2010, de 19 de julio de 2010, FJ 5º.

lía, Policía Judicial y de las partes, al menos; hecho que el Tribunal igualmente podrá considerar en el momento de motivar su decisión de preservar los registros.

El paso del tiempo no conlleva por sí mismo la destrucción de los registros. Esta debe llevarse a cabo mediante una resolución de forma motivada, apreciando las circunstancias concomitantes, y susceptible de ser recurrida. Consecuentemente, los Fiscales deben solicitar en sus escritos de conclusiones provisionales que se manifieste expresamente en las sentencias un veredicto sobre la destrucción; en el caso de sentencias condenatorias, deberá pronunciarse sobre la destrucción de los registros originales y, si por el contrario la sentencia es absolutoria, deberá expresarse tanto de los registros originales como de las copias, excepto cuando sea procedente su conservación. En cuanto a los autos de prescripción o sobreseimiento, se pedirá la destrucción tanto de los registros originales como de las copias.

Hay que aclarar una posible duda en cuanto a la sentencia condenatoria, y es si la destrucción irreversible de las copias de los registros debe ser estipulada en la sentencia por el Tribunal (con efecto aplazado y sujeto al paso de los 5 años desde que se extinga la pena) o debe ser estipulada de forma directa mediante el auto que acuerde dicha extinción. Siguiendo el discernimiento más parejo a la ley, la segunda alternativa parece la más acertada y proporciona una apreciación mejor sobre las posibles circunstancias concomitantes, por si el Tribunal hubiere de suscitar la preservación de los registros.

Sobre quién debe llevar a cabo la destrucción de los registros, haciendo referencia al art. 588 *bis k).3*, prevé que lo haga la Policía Judicial obteniendo primero una orden del Tribunal correspondiente. Sin embargo, no hay ningún impedimento en que pueda realizarlo cualquier persona o entidad que se encuentre en una posición privilegiada, lo cual podría darse cuando los registros originales se encuentren en custodia de alguna entidad colaboradora de la Administración de Justicia y no de la policía, o cuando haya suscrito un convenio de colaboración con otras administraciones o entidades para la destrucción de documentación del Juzgado.

La conservación de los registros, una vez finalizado el propósito que justificaba la medida, podría fundamentarse en motivos históricos, tales como la posibilidad de que concurran otros responsables del delito que no han sido aún juzgados, conflictos técni-

cos para llevar a cabo la destrucción de ciertos registros, que sea necesaria la preservación de registros con una finalidad relativa a inteligencia policial para los supuestos más graves de actividades delictivas, como delitos de terrorismo o, como señalábamos anteriormente, la pendencia de otros recursos, como el recurso de amparo, revisión o ante el Tribunal Europeo de Derechos Humanos.

4.1.4 Contenido de la medida

Grabación y captación de imágenes, es la respuesta que aporta el art. 588 *quinquis a)*. Por captar se asume el visionado y la vigilancia de la escena en tiempo real, a la vez que la grabación conserva una escena semejante.

La diferencia solo es apreciable a nivel de afectación de derechos fundamentales de la persona investigada. Mientras que la captación de la imagen no los menoscaba, la preservación de lo captado mediante la grabación supone que se almacenen una serie de datos de carácter personal que sí pueden afectarlos.

La grabación sólo puede ser de imágenes, pero no incluir sonido, por lo que será irrelevante que la primera se realice en un lugar público, porque para grabar también el sonido habrán de aplicarse los preceptos 588 *quater a)* a *quater e).*

4.1.5 Afectación de terceros

La regla general es que la medida solo afecta a la persona investigada, pero esto puede cambiar en dos ocasiones. La primera, cuando pueda menguar notablemente la vigilancia; en este caso habrá que añadir los casos en los que no resulte posible tomar imágenes de la persona investigada sin que aparezcan otros sujetos, y sin perjudicar la investigación. La segunda ocasión es cuando se prevea que hay indicios fundados de que existan relaciones de otras personas con el investigado o investigada; aquí pues, cuando participen con este en una reunión de la que pueda deducirse una naturaleza delictiva, podrán ser grabadas.

En ambos casos se deberá justificar el razonamiento utilizado para no seguir la regla general, siendo necesaria una explicación y motivación de las circunstancias en el

correspondiente oficio policial que vaya junto con la entrega de las imágenes en el juzgado, excepto cuando del visionado de la grabación se refleje de forma incuestionable el por qué se ha incluido a las personas no investigadas.

4.1.6 Incorporación de la prueba al acto del juicio oral y su valoración

Las filmaciones videográficas realizadas tienen valor probatorio bastante para desvirtuar la presunción de inocencia bajo el requisito de visualización cuando se lleve a cabo el juicio oral, *"para que tengan realidad los principios procesales de contradicción, igualdad, inmediación y publicidad"*[76].

A pesar de ello, es imprescindible que se activen las inspecciones oportunas para agotar cualquier riesgo de modificación o manipulación del material videográfico conseguido, para poder certificar su autenticidad. Para la consecución de este objetivo, y cuando sea posible, deberá llevarse a cabo la confrontación de lo grabado *"con el testimonio en el acto del juicio oral del operador que la obtuvo y fue testigo directo de la misma escena que filmó"*[77]; empero esta última exigencia no será necesaria cuando la grabación no haya sido realizada por una persona, *"sino por las cámaras de seguridad de las entidades que, por prescripción legal, o por iniciativa propia, disponen de esos medios técnicos que graban de manera automática las incidencias que suceden en su campo de acción"*[78].

La Sala de lo Penal del Tribunal Supremo ha aceptado la validez como prueba de las grabaciones videográficas realizadas por medios de comunicación, aunque en su ejecución no existiera, por razones evidentes, ningún control judicial y aunque sean parciales respecto a la totalidad de los hechos ocurridos. Es cierto que, aunque en algunas sentencias se ha exigido la remisión de la filmación en su totalidad, sobre todo cuando se realiza por la Policía, la grabación de momentos precisos por, en este caso, el cámara de televisión, aporta un valor de apreciación de ciertos hechos muy relevante, como la identificación y acreditación de que, en el lugar de los hechos y en el momento tempo-

[76] STS 990/2016, de 12 enero 2017, FJ 12º; STS 124/2014, de 3 febrero 2014, FJ 3º.
[77] STS 1154/2010, de 12 enero 2011, FJ 1.2; STS 990/2016, de 12 enero 2017, FJ 12º.
[78] STS 124/2014, de 3 febrero 2014, FJ 3º; STS 485/2013 de 5 de junio, FJ 2º; STS 67/2014 de 28 de enero, FJ 2º.

ral, las personas en cuestión formaban parte del grupo que ejecutó la conducta reprochable[79].

A continuación haré unas breves apreciaciones jurisprudenciales sobre el valor que debe darse a la grabación videográfica como prueba.

La grabación videográfica no supone una prueba distinta de la percepción visual de una persona, ya que lo único que hace es perpetuarla. Cuando la filmación no se realice por una persona, sino por cámaras de videovigilancia de seguridad que graban de manera automática, es considerada por el Tribunal Supremo como prueba de cargo idónea para desvirtuar la presunción de inocencia. Así mismo, dichas grabaciones se sitúan más cerca de la prueba directa que de la indiciaria, al constituir una evidencia mecánica y objetiva, que excluye el factor humano subjetivo[80].

Para certificar la participación de una persona acusada en el ilícito, basta con que el Tribunal verifique que la grabación se equipara con lo sucedido, ya sea mediante él mismo, mediante funcionarios policiales o testigos[81]; es valorable que, a consecuencia de la percepción o visualización directa del Tribunal de la grabación, se identifique al autor del hecho como el acusado presente en el juicio[82].

4.2 Utilización de dispositivos técnicos de seguimiento y de localización

Su manejo se prevé y regula para la investigación de comportamientos delictivos en los artículos 588 *quinquies b)* y 588 *quinquies c)* de la LECRIM, tratándose de las "balizas", cuyo uso ya se empleaba hace unos años. Dicho presupuesto comprenderá solo a los dispositivos técnicos que incluyan la geolocalización, pero no la imagen ni el sonido; todo ello en el marco de una investigación criminal, como la medida anterior.

El preámbulo de la LOMLECRIM define la necesidad de regulación de esta medida, por la importancia que puede llegar a tener el hecho de que los poderes públicos conozcan la ubicación espacial de cualquier persona; el TEDH considera que puede

[79] STS 1154/2010, de 12 enero 2011, FJ 1.3º.
[80] STS 134/2017, de 2 marzo, FJ 4º.
[81] STS 1336/1999, de 15 septiembre, FJ Único (Recurso de Jon).
[82] STS 1665/2001, de 28 de septiembre, FJ 1º.

conllevar una intromisión en la vida privada de la persona investigada, que, en ocasiones, puede vulnerar el artículo 8 del CEDH; esta es una de las causas por las cuales en virtud del art. 588 *quinquies b).1,* la nueva regulación contempla la autorización judicial[83] tanto para la utilización como para la colocación del dispositivo. En los casos de urgencia, cuando la última se lleve a cabo policialmente según el apartado 4 del mismo art., es importante que el Juez ratifique la medida de la colocación o su cese, ya que, en este último caso, significará que la información lograda carecerá de efectos en el proceso. Se desprende del apartado 3 y del 588 *bis b)* que esta medida podrá ser solicitada por la Policía Judicial o por el Ministerio Fiscal, pudiendo ser también adoptada de oficio por el propio Juez.

4.2.1 Clases y su distinto tratamiento

La geolocalización es posible mediante dispositivos técnicos basados en sistemas de posicionamiento global, como el GPS, y también mediante datos electrónicos asociados a sistemas de comunicación telefónica.

Los primeros son los más aprovechados y permiten vigilar los desplazamientos y ubicaciones de la persona investigada mediante el uso de un dispositivo GPS o análogo, controlado por la Policía Judicial y que será instalado en un vehículo o en otro objeto que aquél tenga en su poder; son los denominados dispositivos técnicos de seguimiento y localización, según el art. 588 *quinquies b).* En estos casos la Policía Judicial se encarga de obtener los datos sobre el posicionamiento que sean generados por el dispositivo y de dirigir al Juez de Instrucción el oficio acordando la medida.

Los segundos obtienen los datos de localización del sistema global para las comunicaciones móviles o GSM[84] que produzca el dispositivo de telefonía móvil de la persona investigada, que se encontraran en manos de la compañía de telecomunicaciones; se trata de los medios técnicos de seguimiento y localización. El oficio, en este supuesto, será dirigido a dichas compañías, exceptuando el caso en el que se haya acordado por resolución judicial la intervención de comunicaciones telefónicas.

[83] AGUSTINA SALLEHÍ, J.R.: *Sobre la utilización oculta de GPS en investigaciones criminales y detección de fraudes laborales,* La Ley Penal nº 102, mayo-junio 2013, Madrid, pp, 21 a 29.
[84] Del inglés "Global System for Mobile Communications", en castellano, sistema global de comunicaciones.

4.2.1.1 Supuesto excluido

El único supuesto que elude esta regulación será cuando se quiera obtener datos de geolocalización de fechas anteriores. La solución es, para cuando se procure el registro de dispositivos técnicos, la aplicación de los arts. 588 *sexies a)* y siguientes, que señalan, en términos generales, que será necesaria la resolución del Juez de Instrucción que autorice el acceso a la información que contienen los dispositivos, limitando los términos y el alcance del registro y que podrá también permitir que se hagan copias de los datos informáticos.

A su vez, cuando se trate de conseguir datos de medios técnicos que se encuentren en los archivos automatizados de los prestadores de servicios o personas que proporcionen comunicaciones cumpliendo las leyes sobre datos relativos a comunicaciones electrónicas, se habrá de estar a lo dispuesto en el art. 588 *ter j),* que establece que los datos solo podrán ser cedidos para su incorporación al proceso con autorización judicial.

4.2.2 Sujetos obligados a la colaboración

Todos los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o servicios de la sociedad de la información, así como cualquier otra persona que pueda aportar información, están obligados a prestar al Juez, al Ministerio Fiscal y a los agentes de la Policía Judicial que hayan sido designados para la práctica de la medida, la asistencia y colaboración que sea necesaria para facilitar la consecución de los autos que ordenen el seguimiento, en virtud todo ello de los arts. 588 *ter e)* y 588 *quinquies b)*.3; los sujetos a los que se emplace para prestar colaboración tienen la obligación de guardar secreto respecto a las actividades requeridas por las autoridades, bajo advertencia de incurrir en un delito de desobediencia.

El supuesto práctico más común se producirá cuando las vigilancias se realicen a través de localización GSM, pues los datos de esta se encuentran custodiados por las compañías de telecomunicaciones.

Por otro lado, al hablar de personas ajenas a los procesos de comunicación telefónica que deben colaborar también, podrían servir de ejemplo los fabricantes de vehículos, que son los que instalan los sistemas de geolocalización y los que pueden facilitar los medios para acceder a la información contenida en el dispositivo colocado en el vehículo para su seguimiento en el supuesto de robo. La falta de un precepto específico que prevea el delito de desobediencia para estos sujetos no es obstáculo para su imputación a tenor del art. 118 CE, que expresa la obligación de prestar la colaboración requerida por Jueces y Tribunales en el curso del proceso y en la ejecución de lo resuelto. Por tanto, la negativa de cualquier persona que pudiera ayudar a la ejecución de la diligencia de investigación, puede llegar a ser suficiente para la imputación de tal delito.

4.2.3 Requisitos

Para poder utilizar los dispositivos o medios técnicos de seguimientos, deberán cumplirse las siguientes condiciones.

4.2.3.1 Concurrencia de principios rectores

En primer lugar, el art. 588 *quinquies b)* supedita lo anterior al cumplimiento de los principios de necesidad y proporcionalidad, específicamente, pero también a los de especialidad, idoneidad y excepcionalidad, señalados de forma general en el art. 588 *bis a).* Por ende, la resolución judicial que habilite la medida fundamentará que la misma se va a utilizar para la investigación de un delito concreto (especialidad), siendo adecuada para la persona investigada y durante el tiempo que sea indispensable (idoneidad), no pudiendo aplicarse otra técnica de investigación más cuidadosa que ésta para el correcto aprecio a los derechos fundamentales (excepcionalidad).

El principio de necesidad pretenderá que la investigación muestre que el uso de estos dispositivos o medios técnicos favorece el avance del descubrimiento de los comportamientos delictivos que se están indagando, aportando datos e indicios precisos y objetivos. La resolución judicial habilitante debe aunar todo ello, más la explicación de la necesidad de uso de la medida para los fines de la investigación.

El principio de proporcionalidad requerirá un juicio de ponderación en la resolución judicial que resuelva que los beneficios de la aplicación de la medida para la investigación son superiores a la limitación que se pueda llegar a dar en el derecho a la intimidad de la persona investigada.

Un factor muy importante para este principio es la duración de la medida, pues la recopilación sistemática de datos de geolocalización dilatada en el tiempo hace que, cuanto más dure, la limitación del derecho fundamental a la intimidad de la persona investigada será directamente proporcional, y aumentará la injerencia al recabar una mayor cantidad de datos, que si se recopilase uno solo, pues *"la gravedad de la injerencia se produce por la monitorización continuada de la geolocalización constante y de la información privada que la misma desprende del investigado"* [85], según el Tribunal Europeo de Derechos Humanos; por su parte, la jurisprudencia norteamericana dictamina que *"son la intensidad de la injerencia y el factor tiempo los que hacen que la medida afecte claramente a esa expectativa razonable de privacidad"*[86].

En definitiva, y como señala el Tribunal Supremo, *"la afectación a la intimidad habrá de graduarse conforme a los factores y circunstancias concurrentes en cada caso, y recordando la necesidad de un permanente ajuste al principio de proporcionalidad en la triple vertiente de adecuación, necesidad y proporcionalidad en sentido estricto"*[87].

4.2.3.2 Juez competente

Este apartado requiere precisiones, pues el Juez competente que está habilitado para adoptar la medida deberá hacerlo en muchos casos aun cuando no exista un procedimiento judicial. La especialidad reside en que los seguimientos policiales son los que facilitan la compilación de hechos suficientes como para la iniciación de aquél; ello supone que, a la vez que el Juez resuelve sobre si acuerda la medida, también analiza si tiene competencia.

[85] STEDH de 4 mayo de 2000, caso Rotaru contra Rumanía; STEDH de 15 febrero 2000, caso Amman contra Suiza (lo dice la STS 610/2016, de 7 julio, FJ 1º).
[86] Sentencia de la Corte Suprema de 23 de enero de 2012 (caso Estados Unidos contra Antoine Jones, 565 US, 2012).
[87] STS n.º 610/2016, de 7 de julio, FJ 1º.

En virtud del art. 14 LECRIM y la doctrina de la ubicuidad[88] del Tribunal Supremo, la medida deberá instarse al Juez de Instrucción del partido judicial donde el delito se haya cometido o de aquel en cuya circunscripción se hayan perpetrado o se estén realizando alguno de los elementos del tipo, sin perjuicio de los delitos cuya competencia se atribuya a la Audiencia Nacional o a otros Órganos Judiciales (como sería el caso de los aforados), en los que la medida deberá solicitarse de ellos.

Habrá casos en los que el Juez competente coincidirá con el del lugar donde se halle el objeto en el que va a ser colocado el dispositivo, si en ese partido judicial se están produciendo actos que componen el tipo penal, por ejemplo, cuando se pretenda colocar un dispositivo en un vehículo que esté siendo utilizado por la persona investigada para mantener encuentros preparatorios de su actividad delictiva. No obstante, cuando el delito se esté produciendo en lugar diferente de aquel en el que se halle el objeto que va a ser vigilado, se habrá de acudir al Juez correspondiente al primero.

Sea como fuere, en caso de que la solicitud se presente ante un Juez que no es competente territorialmente, siguiendo el criterio de los arts. 12 y 13 LECRIM, se deberá analizar si la medida de investigación es imprescindible para la consignación de pruebas del delito que tengan riesgo de desaparición. Si lo hay, el Juez deberá decidir lo procedente sobre la medida requerida, acordando posteriormente su inhibición al Juez competente; si no hay riesgo, podrá inhibirse directamente sin entrar a resolver sobre la medida.

4.2.3.3. Especificación del medio técnico que vaya a ser utilizado

Este requisito deberá ser incluido en la autorización judicial, en virtud del art. 588 *quinquies b).2,* y solo existe esta referencia específica acerca del contenido de aquélla en la regulación. Teniendo en cuenta los arts. 588 *bis c.3.b)* y 588 bis *c.3.g),* se desprende que el Juez habría de mencionar además la identidad de la persona investigada y cualquier otra persona afectada por la medida, porque sobre ellos o sus bienes vaya a

[88] *"Respecto del lugar en el que debe entenderse cometido el delito, la Jurisprudencia de esta tiene señalado que debe venir fijado a través de la llamada teoría de la ubicuidad, esto es, que el delito se consuma en todos los lugares en los que se ha llevado a cabo la acción o en el lugar en el que se haya producido el resultado"* (STS 504/2016, de 9 junio 2016, FJ 1º; STS 798/2013, FJ 3º; STS 1/2008, de 23 de enero de 2008, FJ Único). *"La teoría de la ubicuidad en materia de competencia territorial se ha constituido en la doctrina dominante"* (STS 456/2013, de 9 de junio de 2013, FJ 2º).

colocarse un dispositivo, y el propósito perseguido con la medida. Aunque ello no sea exigible, su indicación debe ser considerada como una forma ineludible para poder analizar la proporcionalidad e idoneidad de la medida, pues la incidencia en el derecho a la intimidad será distinta si el dispositivo se coloca sobre su teléfono móvil o en una embarcación en la que se encuentra, ya que en el primer caso será posible saber todos sus movimientos, y en el segundo, solo podrá observarse la determinada travesía o ruta marina que navegue.

Como hemos mencionado anteriormente, al amparo del art. 588 *bis c.3.b),* el dispositivo puede ser colocado en un objeto que pertenezca a persona distinta de la persona investigada, lo cual requiere que se indique quién es para poder ser apreciado en la resolución judicial habilitante, que tendrá que hacer un mayor hincapié en justificar si se acepta la medida frente a esta tercera no investigada, ya que pueden verse afectados sus derechos fundamentales y deberá cumplirse la exigencia de los principios de proporcionalidad y necesidad.

La mención del medio técnico que quiere emplearse es necesaria para delimitar el alcance de la medida y el grado de limitación del derecho fundamental. Ello se deriva de la precisión; siendo mayor en un dispositivo GPS, pues tiene un margen de error de escasos metros en los datos de posicionamiento que proporciona, mientras que es menor en los datos de posicionamiento de un teléfono, en la localización GSM. Además, en la resolución deberá realizarse un examen exhaustivo de las exigencias que se deriven del tipo de dispositivo que vaya a colocarse, así como en el caso de que resulte imperativo entrar en el domicilio, garaje o vehículo de la persona investigada para la colocación del mismo.

En conclusión, se deberá indicar como mínimo el sistema de vigilancia y localización que vaya a emplearse, el objeto o la persona en que se colocará y cualquier hecho que pudiera ser significativo y limitativo del derecho fundamental a la intimidad. No obstante, no será necesario señalar específicamente el dispositivo a utilizar, ni la ubicación exacta donde vaya a colocarse, pues ello actuaría en detrimento al desvelar las técnicas utilizadas por las unidades policiales, favoreciendo que las personas investigadas adopten medidas para sortear y frustrar el operativo.

4.2.3.4. Otros requisitos derivados de la aplicación de las disposiciones comunes

Uno de los requisitos comunes a todas las medidas de investigación tecnológica es la entrega al Juez de los soportes originales o copias electrónicas auténticas de la información recogida, señalada en el art. 588 *quinquies c).* A su vez se encuentra reseñada de forma general en el art. 588 *bis g)*[89], y referida a la interceptación de comunicaciones telefónicas y telemáticas en el art. 588 *ter f)* [90].

En cuanto a dispositivos técnicos de localización y seguimiento, se hará entrega, generalmente, de copias en formato electrónico de los datos que se hayan obtenido, que podrán provenir de dispositivos GPS o de datos asociados al GSM. En el primer caso, será la Policía Judicial la encargada de la mencionada entrega, en un formato que avale su autenticidad, siendo suficiente cualquier método de sellado homologada. En el segundo caso, serán las compañías que suministran los servicios de comunicación las que remitan los datos, pero aquí la autenticidad se probará mediante protocolos implementados en los sistemas utilizados para la recepción de tales datos, como el SITEL.

Hay que tener en cuenta la necesidad de que la información que ha sido recopilada mediante esta medida sea custodiada adecuadamente, para impedir que sea utilizada indebidamente, siendo necesaria finalmente su destrucción siguiendo las directrices del art. 588 *bis k),* como y vimos en el apartado 4.1.3.3.

4.2.4 Duración de la medida

Continuando con el art. 588 *quinquies c),* en su apartado primero señala que la utilización de la medida de utilización de dispositivos técnicos de seguimiento y localización durará como máximo 3 meses a partir de la fecha de su autorización, pudiendo el

---

[89] *"La Policía Judicial informará al juez de instrucción del desarrollo y los resultados de la medida, en la forma y con la periodicidad que este determine y, en todo caso, cuando por cualquier causa se ponga fin a la misma".*

[90] *"En cumplimiento de lo dispuesto en el artículo 588 bis g, la Policía Judicial pondrá a disposición del juez, con la periodicidad que este determine y en soportes digitales distintos, la transcripción de los pasajes que considere de interés y las grabaciones íntegras realizadas. Se indicará el origen y destino de cada una de ellas y se asegurará, mediante un sistema de sellado o firma electrónica avanzado o sistema de adveración suficientemente fiable, la autenticidad e integridad de la información volcada desde el ordenador central a los soportes digitales en que las comunicaciones hubieran sido grabadas".*

Juez acordar, excepcionalmente, prórrogas sucesivas por un plazo igual o menor, hasta un máximo de 18 meses, si de este modo estuviera justificado a la vista de los resultados obtenidos. Si bien es cierto que el sostenimiento de la medida durante varios meses puede aumentar el nivel de intromisión en la intimidad de la persona investigada, este sostenimiento deberá ser analizado mediante el juicio de proporcionalidad de la resolución judicial que lo acuerde.

Hay que recordar que el inicio del cómputo está fijado para cuando se autorice la medida y no para el momento en que se coloque el dispositivo; esto es transcendental, ya que los datos recabados fuera del plazo autorizado podrán ser declarados nulos como prueba.

Debe tenerse en mente que en el art. 588 *bis f)* se encuentran las exigencias a las que se sujetan las prórrogas. Establece que las solicitudes de éstas serán dirigidas por el Ministerio Fiscal o la Policía Judicial al Juez competente con suficiente anticipación para evitar la expiración del plazo otorgado, debiendo contener un informe minucioso del resultado de la medida y los motivos que justifiquen la continuidad de la misma, según el primer apartado.

El Juez se pronunciará sobre el fin o prórroga de la medida mediante auto motivado, en el plazo de los dos días siguientes a la presentación de la solicitud, pudiendo aquél pedir aclaraciones o mayor información antes de emitir la decisión, conforme al segundo apartado.

Por último, en el tercer apartado observamos que, una vez el Juez haya autorizado la prórroga, el inicio del cómputo de esta será desde la fecha de expiración del plazo de la medida acordada.

4.2.5. Adopción policial de la medida en casos de urgencia

Se ha incorporado a la Ley mediante el art. 588 *quinquies b).4*, la doctrina que ya instauró el Tribunal Constitucional: *"si ex art. 18.3 CE*[91] *la intervención de las co-*

[91] *"Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial".*

municaciones requiere siempre resolución judicial, no existe en la Constitución reserva absoluta de previa resolución judicial respecto del derecho a la intimidad personal, de modo que excepcionalmente hemos admitido la legitimidad constitucional de que en determinados casos y con la suficiente y precisa habilitación legal la policía judicial realice determinadas prácticas que constituyan una injerencia leve en la intimidad de las personas, siempre que se hayan respetado las exigencias dimanantes del principio de proporcionalidad"[92]*; "Precisando la anterior doctrina, hemos venido estableciendo como requisitos que proporcionan una justificación constitucional objetiva y razonable a la injerencia policial en el derecho a la intimidad (art. 18.1 CE), los siguientes: a) la existencia de un fin constitucionalmente legítimo, considerando como tal el interés público propio de la prevención e investigación del delito, y, más en concreto, la determinación de hechos relevantes para el proceso penal; b) que la medida limitativa del derecho a la intimidad esté prevista en la ley (principio de legalidad); c) que, en caso de no contar con autorización judicial (o consentimiento del afectado), la actuación policial se atenga a la habilitación legal, teniendo en cuenta que la ley puede autorizar a la policía la práctica de inspecciones, reconocimientos e incluso intervenciones corporales leves, siempre y cuando se respete el principio de proporcionalidad, concretado en tres exigencias o condiciones: idoneidad de la medida, necesidad de la misma y juicio de proporcionalidad en sentido estricto"*[93].

Como conclusión de la doctrina, teniendo en cuenta la menor intensidad de la intromisión en el derecho fundamental, y que no existe reserva constitucional acerca del derecho a la intimidad, hay que observar que la Ley ha previsto una excepción a la regla general sobre la necesidad de previa habilitación judicial para la adopción de la medida, y se encuentra en el apartado 4 del art. 588 *quinquies b)*. Establece que la Policía Judicial podrá proceder a la colocación inmediata de un dispositivo o medio técnico de seguimiento o localización cuando existan razones de urgencia que permitan temer que, de no colocarlo inmediatamente, la investigación se verá frustrada. Aquélla deberá informar a la autoridad judicial de este hecho en el plazo más breve posible, y en todo caso, en 24 horas como límite máximo; esta podrá ratificar la medida adoptada o acor-

[92] Sala Primera. STC 281/2006, de 9 de octubre (BOE núm. 274 de 16 de noviembre de 2006), FJ 3º; STS 610/2016, de 7 de julio, FJ 1º.
[93] STS 610/2016, de 7 de julio, FJ 1º; Sala Segunda. STC 173/2011, de 7 de noviembre (BOE núm. 294 de 07 de diciembre de 2011); Sala Primera. STC 70/2002, de 3 de abril (BOE núm. 99 de 25 de abril de 2002), FJ 10º.

dar su cese inmediato en el mismo plazo. En este último caso, la información que se haya recopilado del dispositivo colocado carecerá de valor en el proceso.

La urgencia será visible en los supuestos en los que el plazo de tiempo del que se dispone para la colocación del dispositivo no permita solicitar autorización de la autoridad judicial; a modo de ejemplo, durante un seguimiento que se le esté realizando a la persona investigada, si este contacta con otro sospechoso que también se quiere vigilar y no haya en el momento efectivos policiales disponibles, no habrá tiempo materialmente posible para solicitar a la autoridad la instalación del dispositivo en el vehículo del sospechoso.

Por su parte, el principio de necesidad ordenará la acreditación de que, de no llevarse a cabo el seguimiento y localización por medio del dispositivo técnico, pudiera malograrse la investigación. La valoración de la urgencia y necesidad de la medida debe hacerse ex ante por la Policía Judicial, cuando vaya a adoptarse, y no después teniendo en cuenta los resultados, y ello viene justificado por el Tribunal Constitucional, que establece que sobre aquella valoración se puede realizar un control judicial ex post, pero que si en él se verifica *"la falta del presupuesto habilitante o del respeto al principio de proporcionalidad, implicaría la vulneración del derecho fundamental y tendría efectos procesales en cuanto a la ilicitud de la prueba en su caso obtenida, por haberlo sido con vulneración de derechos fundamentales"*[94].

Será imprescindible, pues, que exista situación de urgencia y necesidad estricta de la medida, debiéndose justificar posteriormente en el oficio que la Policía Judicial presente ante el Juez competente para que ratifique la medida. Ello hace posible además que la prueba que resulte de la colocación del dispositivo pueda ser considerada como válida. Para acreditar el cumplimiento de los plazos del apartado 4 del art. 588 *quinquies b)*, mencionado supra, se recomienda que en el oficio se haga constar tanto la hora concreta de la instalación del dispositivo como de la presentación del oficio en el Juzgado.

[94] STC 70/2002, de 3 de abril (BOE núm. 99 de 25 de abril de 2002), FJ 10º.

La ratificación se hará mediante auto en el que el Juez justificará y motivará la procedencia de la medida, y validará la actuación policial admitiendo la concurrencia de los requisitos, lo cual significará que existía la urgencia en el momento de la adopción de la medida y la necesidad estricta que de ella se derivaba, así como que le fue dada cuenta de su adopción en plazo. Para resolver cuenta, con carácter general, con el tiempo que se establece en el apartado 1 del art. 588 *bis c),* es decir, 24 horas, computándose desde el momento en que la Policía Judicial presente el oficio al Juez.

Si se incumplen los plazos fijados o no se acredita la urgencia o posible frustración de la investigación de no haberse adoptado la medida, podrá producirse la nulidad de los datos de geolocalización recopilados por el dispositivo técnico que se instaló; ello no impide que, de forma posterior, el Juez autorice la misma medida incorporando lícitamente al procedimiento los datos que transmita el dispositivo que fue instalado desde el momento de esa autorización.

4.2.6 Supuestos de geolocalización no incluidos en la regulación legal

Cuando la Policía Judicial está investigando un delito y utiliza un dispositivo técnico, pero no para seguir a una persona, sino a un objeto, no se encuentra sujeta a la exigencia de previa habilitación judicial del art. 588 *quinquies a),* ya que de este modo no se menoscaba derecho fundamental alguno.

Este es el caso de los paquetes postales o contenedores de mercancías, ya que el dispositivo técnico informará sobre la ruta que sigan aquéllos y sobre su localización concreta en cada momento, pero no información de personas determinadas, lo que hace que el Tribunal Supremo establezca que hay una diferencia *"si el dispositivo GPS es aplicado directamente sobre objetos, para su localización, o para la localización de personas"*[95], pues solo en el último caso es posible la afectación del derecho a la intimidad.

Puede darse la circunstancia de que el seguimiento del objeto se dilate un tiempo tras haber sido retirado por una persona en concreto, por lo que se podría poner en tela

[95] STS 610/2016, de 7 de julio, FJ 1º.

de juicio si se ha visto invadida la intimidad de esta; sin embargo, solo podrá plantearse la duda en el supuesto de que los datos de geolocalización puedan relacionarse con la persona si fuera identificada.

Lo mismo ocurre en el caso del seguimiento y localización de medios de transporte. El Tribunal Supremo ha señalado que la colocación de una baliza en una embarcación permitió su seguimiento y controlar su ubicación, y para instalarla en los exteriores de la misma no se realizó intromisión alguna en la intimidad, por lo que no se solicitó intervención judicial; se trata de una diligencia de investigación, legítima desde la función constitucional atribuida a la Policía Judicial[96]. No obstante, ello ha de ser matizado, pues la autorización judicial sí que será necesaria cuando sea relevante para la investigación la identificación de sus tripulantes o cuando esta vaya a ser utilizada de alguna forma en el procedimiento, afectando el derecho a la intimidad de aquéllos.

[96] STS 562/2007, de 22 de junio, FJ 2º; STS 798/2013, de 5 de noviembre, FJ 11º; STS 610/2016, de 7 de julio, FJ 1º.

CONCLUSIONES

Primera. La posible afectación que produce la aplicación de las medidas de investigación tecnológica a los Derechos Fundamentales, como son el derecho a la intimidad (art. 18.1 CE), el derecho al secreto de las comunicaciones (art. 18.3 CE) y el derecho al entorno virtual, denominado así por la jurisprudencia más temprana, y más tarde, como derecho a la protección de datos, contenido en el art. 18.4 CE, ha sido digna de ser estudiada conforme a los criterios que establecen los Tribunales, pues solo así es posible comprender las limitaciones y la justificación que estos aportan a los casos reales. Así mismo, es importantísimo valorar la doctrina consolidada sobre los derechos apuntados supra, para que puedan apreciarse las pruebas obtenidas de las mencionadas medidas, porque de lo contrario podrían declararse ilícitas y, en caso de ser la única prueba a tener en cuenta, la persona investigada podría quedar impune del ilícito cometido.

Segunda. El Estado tendía a invadir en sus tareas de investigación de los delitos ese derecho al entorno digital, en su deber legítimo de condenar los mismos, pues al principio ese concepto no se contemplaba con la importancia que merece y no estaba muy claro; según los Tribunales, el entorno virtual es un espacio digital donde habitualmente se ejercitan los derechos fundamentales mencionados, como la intimidad, las comunicaciones y la protección de datos. Por su parte, este último derecho, relacionado con el derecho al entorno digital pero siendo distinto de aquél, supone la autodeterminación informativa y *habeas data*, que nos permite tener un derecho sobre los datos personales que un tercero posee de nosotros, no pudiendo ese tercero tenerlos sin nuestro consentimiento, ni utilizarlos para un propósito distinto para el que fueron recogidos, ni cederlo a otros sin nuestra aquiescencia, y, además, podemos ejercer lo que se denomina el *habeas data*, si no fuese así.

Tercera. La LOMLECRIM es digna de mención al adecuar la parca legislación existente hasta el momento a nuevas formas de comisión de delitos derivadas del uso de las nuevas tecnologías añadiendo a la LECRIM, en su Título VIII del Libro II, un nuevo capítulo, el VII. Su contenido es el objeto de este trabajo, la utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización, encontrándose las disposiciones comunes a estas medidas en la reciente *Circular 1/2019.* En esta última

regulación encontramos muchas de las exigencias que los Tribunales venían demandando regular, y que ha satisfecho de manera fehaciente la Fiscalía General de Estado.

Cuarto. De igual manera, las medidas analizadas en el trabajo se ven detalladas y extensamente contenidas en la *Circular 4/2019.* La captación de imágenes ha de ser en lugares o espacios públicos, comprendiendo únicamente el campo visual y no se permite la grabación de sonido; lo mismo sucede con los dispositivos de geolocalización, pero en este caso no permite la filmación de imagen. La adopción de la primera medida exige que sea indispensable para proporcionar la identificación de la persona investigada, para localizar las herramientas o instrumentos del delito u obtener datos que tengan relevancia para aclarar los hechos. La segunda es imprescindible cuando se pretende realizar un seguimiento del investigado, debiendo conocer para ello su ubicación. Son medidas altamente eficaces y aplicadas de forma continua por la Policía Judicial, siendo, en mi opinión, un avance muy satisfactorio para poder perseguir los delitos que surgen del uso de las nuevas tecnologías.

BIBLIOGRAFÍA

- **ARMENTA DEU, T.:** *Lecciones de Derecho Procesal Penal,* Editorial Marcial Pons, 9º edición, Madrid 2016.
- **AGUSTINA SANLLEHÍ, J.R.:** *Sobre la utilización oculta de GPS en investigaciones criminales y detección de fraudes laborales,* en la Revista La Ley Penal, n 102, mayo-junio 2013, pp. 21 a 29.
- **DÍAZ MARTÍNEZ, M.; GIMENO SENDRA, V.:** *Derecho Procesal Penal (para policías y criminólogos).* Ed. Edisofer, Madrid, 2018.
- **GARCIMARTÍN MONTERO, R.:** *Los medios de investigación tecnológicos en el proceso penal,* Ed. Aranzadi, Cizur Menor (Navarra), 2018.
- **MESTRE DELGADO, E.:** *La intimidad, devaluada frente a la investigación de delitos,* Diario La Ley de 17 mayo de 2013.
- **TOMÉ GARCIA, J.A.:** *Curso de Derecho Procesal penal,* Madrid, 2016.
- **ZOCO ZABALA, C.:** *Nuevas tecnologías y control de las comunicaciones.* Editorial Aranzadi, S.A., Pamplona (Navarra), Primera edición, 2015.

LEGISLACIÓN

- *Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen,* «BOE» núm. 115, de 14 de mayo de 1982.
- *Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos,* «BOE» núm. 186, de 5 de agosto de 1997.
- *Ley Orgánica 13/2015 de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica,* «BOE» núm. 239, de 6 de octubre de 2015.
- *Ley 5/2014, de 4 de abril, de Seguridad Privada,* «BOE» núm. 83, de 5 de abril de 2014.
- *Real Decreto 596/1999, de 16 de abril, por el que se aprueba el Reglamento de desarrollo y ejecución de la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos,* «BOE» núm. 93, de 19 de abril de 1999.

- *Real Decreto 424/2005, de 15 de abril, por el que se aprobó el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas y el servicio universal y la protección de los usuarios*, «BOE» núm. 102, de 29 de abril de 2005.

OTROS DOCUMENTOS JURÍDICOS:

- Circular 1/2019, de 6 de marzo, de la FGE, sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológicas en la LECR.
- Circular 4/2019, de 6 de marzo, de la FGE, sobre utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización.

JURISPRUDENCIA DEL TRIBUNAL CONSTITUCIONAL

- Pleno. STC 11/1981, de 8 de abril (BOE núm. 99 de 25 de abril de 1981).
- Sala Segunda. STC 114/1984, de 29 de noviembre (BOE núm. 305 de 21 de diciembre de 1984).
- Sala Segunda. STC 231/1988, de 2 de diciembre (BOE núm. 307 de 23 de diciembre de 1988).
- Sala Segunda. STC 144/1999, de 22 de julio (BOE núm. 204 de 22 de agosto de 1999).
- Sala Segunda. STC 115/2000, de 5 de mayo (BOE núm. 136 de 7 de junio de 2000).
- Pleno. STC 290/2000, de 30 de noviembre (BOE núm. 4 de 4 de enero de 2001).
- Pleno. STC 292/2000, de 30 de noviembre (BOE núm. 4 de 4 de enero de 2001).
- Sala Primera. STC 70/2002, de 3 de abril (BOE núm. 99 de 25 de abril de 2002).
- Sala Primera. STC 281/2006, de 9 de octubre (BOE núm. 274 de 16 de noviembre de 2006).
- Sala Segunda. STC 173/2011, de 7 de noviembre (BOE núm. 294 de 07 de diciembre de 2011).

- Sala Primera. STC 12/2012, de 30 de enero (BOE núm. 47 de 24 de febrero de 2012).
- Sala Primera. STC 74/2012, de 16 de abril (BOE núm. 117 de 16 de mayo de 2012).
- Sala Segunda. STC 145/2014, de 22 de septiembre (BOE núm. 261 de 28 de octubre de 2014).

JURISPRUDENCIA TRIBUNAL SUPREMO

- STS 453/1997, de 15 abril.
- STS 968/1998, de 17 julio.
- STS 134/1999, de 15 julio.
- STS 1336/1999, de 15 septiembre.
- STS 1665/2001, de 28 de septiembre.
- STS 354/2003, de 13 marzo
- STS 562/2007, de 22 de junio
- STS 1/2008, de 23 de enero de 2008
- STS 96/2009, de 10 de marzo.
- STS 1154/2010, de 12 enero.
- STS 1154/2010, de 12 enero.
- STS 513/2010, de 2 junio.
- STS 753/2010, de 19 de julio.
- STS 1220/2011, de 11 de noviembre.
- STS 777/2012, de 17 de octubre.
- STS 85/2013, de 4 de febrero.
- STS 342/2013, de 17 de abril.
- STS 456/2013, de 9 de junio.
- STS 485/2013 de 5 de junio
- STS 798/2013, de 5 de noviembre.
- STS 67/2014 de 28 de enero.
- STS 124/2014, de 3 febrero.
- STC 157/2014, de 5 de marzo.
- STS 239/2014, de 1 de abril.
- STS 528/2014, de 16 de junio.
- STS 587/2014, de 18 de julio.

- STS 329/2016, de 20 abril.
- STS 990/2016, de 12 enero 2017
- STS 329/2016, de 20 abril.
- STS 504/2016, de 9 junio.
- STS 610/2016, de 7 de julio.
- STS 610/2016, de 7 de julio.
- STS 134/2017, de 2 marzo.
- STS 200/2017, de 27 marzo.
- STS 287/2017, de 19 de abril
- STS 788/2017, de 7 de diciembre.
- STS 489/2018, de 23 de octubre.
- STS 427/2019, de 26 de septiembre.
- STS 554/2019, de 13 de noviembre.

JURISPRUDENCIA DEL TRIBUNAL EUROPEO DE DERECHOS HUMANOS

- STEDH de 15 febrero 2000, caso Amman contra Suiza.
- STEDH de 15 febrero 2000, caso Amman contra Suiza; STEDH de 4 mayo de 2000, caso Rotaru contra Rumanía.
- STEDH, de 9 de enero de 2018, asunto López Ribalda y otros contra España.
- Sentencia de la Gran Sala del Tribunal Europeo de Derechos Humanos, de 17 de octubre de 2019, asunto López Ribalda y otros contra España.